공기업정책학 석사 학위논문

정보보안 스트레스 요인에 관한 연구

- K공사 사례를 중심으로 -

2013년 8월

서울대학교 행정대학원

공기업정책학과

유 승 민

정보보안 스트레스 요인에 관한 연구

- K공사 사례를 중심으로 -

지도교수 우 지 숙

이 논문을 공기업정책학 석사 학위논문으로 제출함

2013년 5월

서울대학교 대학원

공기업정책학과

유 승 민

유승민의 석사 학위논문을 인준함

2013년 6월

위 원 장 김 봉 환 (인)

부위원장 권 혁 주 (인)

위 원 우 지 숙 (인)

국문초록

본 연구의 목적은 조직성원들이 체감하는 정보보안 스트레스에 영향을 미치는 요인을 분석하고, 스트레스를 최소화할 수 있는 방안을 제시하여 효율적인 정보보안 정책 수립에 도움이 되는 것이다.

이를 위해 K공사의 본사 및 3개 사업본부를 대상으로 설문조사를 하여 240여개의 유효한 자료를 확보하였다. 또한 자료 분석을 위해 빈도분석, 신뢰도 분석, 요인분석, 상관관계 분석 및 다중회귀분석을 실시하였다.

이에 따른 본 연구의 분석결과는 아래와 같이 요약할 수 있다.

첫째, 조직구성원의 특성관련 총 6개 요인 중 5개가 기술적 보안 스트레스에 통계적으로 유의미한 부(-)의 영향을 미치는 것으로 나타났다. 세부적으로 살펴보면 본사 근무 여부는 제외하고, 보안관심도, 회사 보안 전략신뢰도, 회사 보안 교육수준, 보안업무 담당 여부, 간부 여부가 부(-)의 영향을 미쳤다. ICT보안업무 종사자와 간부는 일반 사무직 종사자와 일반직원들이 체감하는 기술적 보안 스트레스에 차이가 있음을 인식하고, 향후 최신 보안기술, 소프트웨어, 응용 프로그램 도입 시 좀 더 쉽고, 편리하게 운영・관리될 수 있도록 방안을 수립해야 할 것이다.

둘째, 조직구성원의 특성관련 총 6개 요인 중 6개 모두가 관리적 보안 스트레스에 통계적으로 유의미한 부(-)의 영향을 미치는 것으로 나타났다. 이것은 개인적 요인, 회사환경 요인, 직무특성 요인 등 모든 요인들이 조직구성원들이 체감하는 스트레스를 낮춘다는 의미이다. 국정원, 지식경제부 등에 의한 정보보안 지시사항을 접수 후 보안 이행 계획 및 정책을 수립하는 과정에서 관리적 보안 스트레스 유발을 최소화하기 위해 일방향적 정책 수립이 아닌, ICT보안업무 종사자와 일반 사무직 종사자, 간부와 일반직원, 본사 근무자와 사업소 근무자 간 소통을 통한 양방향적 정책 수립이 필요함을 의미한다.

셋째, 조직구성원의 특성관련 총 6개 요인 중 3개가 물리적 보안 스트레스에 통계적으로 유의미한 부(-)의 영향을 미치는 것으로 나타났다. 세부적으로 살펴보면 보안관심도, 회사 보안 교육 수준, 본사 근무 등 3개 요인은 제외하고, 회사 보안 전략신뢰도, 보안업무 담당 여부, 간부 여부가 부(-)의 영향을 미쳤다. 각 분야별 정보보안 스트레스의 회귀모형에 대한 설명력을 비교해보면 관리적 보안 스트레스 > 기술적 보안 스트레스 > 물리적 보안 스트레스 순으로 물리적 보안 스트레스가 가장 낮음을 알 수 있다. 물리적 보안은 PC, 건물 등에 물리적 접근, 접속 차단의 통제를 통한 극단적인 정보보안 요소이기 때문에 다른 보안 요소보다 기본적으로 스트레스가 높다. ICT보안업무 종사자와 간부는 물리적 보안의 특수성을 고려하여 스트레스를 줄이기 위한 추가적 노력이 필요하다.

이와 같은 결론을 종합해 볼 때, 정보보안 스트레스를 낮추기 위해서는 첫째, 회사 보안 전략 신뢰도 향상 방안을 도출해야 한다. 회사에서 보안 정책 수립 시 업무의 생산성과 보안준수간의 상충관계를 고려한 절충안을 마련하여 보안 준수가 생산성을 하락시킨다는 부정적 인식을 전환시킬 필요가 있다. 둘째, 물리적 보안 스트레스를 최소화하는 방안 도출해야 한다. 최신 ICT기술을 접목하여 물리적 보안 스트레스를 완화해야 할 것이다. 셋째, ICT보안업무 종사자는 일반 사무직 종사자가 체감하는 보안 스트레스에 차이가 있음을 인식해야 한다. ICT보안업무 종사자는 합리적이고 효율적인 보안기술 및 시스템을 도입하여 일반 사무직 종사자가 쉽게 이해할 수 있도록 해석해주는 역할을 수행해야 할 것이다. 그리고 다양한 정보보안 스트레스 요인을 지속적으로 모니터링하고, 이에 대한 효율적인 대처 방안을 지속적으로 찾아나가야 할 것이다.

주요어 : 정보보안, 정보보호, 스트레스, ICT보안, 공공기관, 보안통제
학 번 : 2012-22781

목 차

제 1 장 서론 ····· 1

제 1 절 연구의 목적 및 필요성 ····· 1

제 2 절 연구 방법 ····· 4

제 2 장 이론적 논의 및 선행연구 검토 ····· 5

제 1 절 정보보안에 관한 선행연구 고찰 ····· 5

1. 정보보안의 개념 ····· 5

2. 정보보안의 범위 ····· 10

3. 정보보안 현황 ····· 12

제 3 절 정보보안 통제에 관한 선행연구 고찰 ····· 15

제 4 절 정보보안 스트레스에 관한 선행연구 고찰 ····· 22

제 3 장 연구 모형 및 가설 ····· 31

제 1 절 연구 모형의 설계 ····· 31

1. 연구문제 ····· 31

2. 연구모형 ····· 31

제 2 절 연구 가설의 설정 ····· 34

제 3 절 연구 대상 및 분석방법 ····· 38

1. 연구 대상 및 변수의 정의 ····· 38

가. 연구의 대상 ····· 38

나. 종속변수 : 기술적, 관리적, 물리적 보안 스트레스 ····· 39

다. 독립변수 : 개인적, 회사환경, 직무특성 요인 ····· 41
라. 통제변수 ····· 43
2. 연구 분석방법 ····· 44

제 4 장 분석결과 및 논의 ····· 46
제 1 절 표본의 일반적 특성 ····· 46
제 2 절 척도의 신뢰성과 타당성 검증 ····· 49
1. 신뢰성 분석 ····· 49
2. 타당성 분석 ····· 50
3. 상관관계 분석 ····· 53
제 3 절 가설 검증 ····· 54

제 5 장 결론 ····· 62
제 1 절 연구결과의 요약 ····· 62
제 2 절 연구의 시사점 및 한계점 ····· 65
1. 연구의 시사점 ····· 65
2. 연구의 한계점 ····· 68

참고문헌 ····· 70

표 목차

[표 2-1] 정보자산의 분류 ····· 7
[표 2-2] 정보보안과 정보보호 ····· 9

[표 2-3] 정보보안 요소 항목의 계층적 구조 ····· 11
[표 2-4] 우리나라 주요 정보통신지수 순위 ····· 13
[표 2-5] 2011년 침해사고 접수처리 건수 ····· 15
[표 2-6] ISO 17799의 정보보안 통제 ····· 17
[표 2-7] ISMS 인증 통제 분야 ····· 18
[표 3-1] K공사 정보보안 실태 평가 항목 ····· 40
[표 3-2] 독립변수 설문지의 구성 및 출처 ····· 42
[표 3-3] 연구 변수의 정의 ····· 44
[표 3-4] 연구 분석방법 ····· 45
[표 4-1] 설문대상의 성별 및 결혼여부 ····· 46
[표 4-2] 설문대상의 연령 ····· 47
[표 4-3] 설문대상의 최종학력 및 근무지 ····· 47
[표 4-4] 설문대상의 근무분야 및 직위 ····· 48
[표 4-5] 내적 일관성법에 의한 문항 분석 ····· 50
[표 4-6] 요인분석 결과 (독립변수) ····· 51
[표 4-7] 요인분석 결과 (종속변수) ····· 52
[표 4-8] 측정항목과 측정항목 모집단간의 상관관계 ····· 53
[표 4-9] 개인적 환경, 직무특성 요인이 기술적 보안 스트레스에 미치는 영향····· 55
[표 4-10] 개인적 환경, 직무특성 요인이 관리적 보안 스트레스에 미치는 영향·· 58
[표 4-11] 개인적 환경, 직무특성 요인이 물리적 보안 스트레스에 미치는 영향·· 60
[표 5-1] 연구가설 채택 여부 ····· 63

그림 목차

[그림 2-1] 정보보안 분야 ····· 12
[그림 2-2] 스트레스에 관한 연구 모형 ····· 27
[그림 3-1] 보안 스트레스에 미치는 영향을 측정하기 위한 연구모형·· 33

부록 목차

[부록 1-1] 설문지 ····· 74

제 1 장 서 론

제 1 절 연구의 목적 및 필요성

최근 기업들은 정보통신기술(Information & Communication Technologies)[1]을 도입하여 급격한 환경변화와 무한 경쟁시대에 대한 돌파구를 모색하고 있다. ICT의 활용을 통한 경쟁우위 확보를 위해 기업들의 노력은 조직과 ICT의 관계를 더욱 밀착시켰으며, 결국 ICT시스템이 기업 내에서 더욱 중요한 위치를 점하게 되는 계기가 되었다. ICT의 발전과 시스템의 보급은 많은 부작용을 발생시키고 있다. 국내에서도 기업의 정보보안(Information Security)에 관련된 많은 유출 사건이 언론에 보도되어 경각심이 날로 높아지고 있는 실정이다. 이에 정보의 손실은 조직의 존망을 결정하는 가장 핵심적인 경쟁력이 되었고, 이에 따라 기업의 정보보안은 매우 중요한 요소가 되었다.

하지만, 대부분의 기업들이 정보보안에 대한 대책에 있어 하드웨어 또는 소프트웨어의 도입을 통해 해결하려고 하며, 다른 곳의 보안 대책을 그대로 도입하고 있는 실정이다. 정보보안은 기업이 기업의 문화, 환경 등과 같은 상황적 요인에 대한 중요성을 인식하는 것에서부터 시작되어야만 한다. 기업의 정보와 시스템을 보호하기 위해서는 기술적인 측면보다 관리적인 측면 즉, 효과적인 정책을 세우고 이를 조직 구성원들이 실행할 수 있도록 동기 부여를 하는 것이 중요하다. 정보보안 정책이 존

1) 정보통신기술(Information & Communication Technologies) : 정보 기술(Information Technology)과 통신 기술(Communication Technology)의 합성어로 컴퓨터, 미디어, 영상 기기 등과 같은 정보 기기를 운영 · 관리하는데 필요한 소프트웨어 기술과, 이들 기술을 이용하여 정보를 수집 · 생산 · 가공 · 보존 · 전달 · 활용하는 모든 방법을 말한다.

재한다고 해서 모든 조직 구성원이 항상 존중할 것으로 생각하면 잘못이다. 구성원은 왜 이러한 보안정책이 필요한지 이해가 안 되면 정책을 무시하는 경향이 있고, 때로는 반발하기도 하며 이것으로 인해 스트레스를 받기도 한다.

기업들은 자신의 기업에 맞는 보안 기술이 아니라 가격효율성을 고려하여 상용화 패키지를 구입하는 경우가 많다. 이 경우 조직의 환경 및 조직이 지금까지 사용하고 있는 시스템과의 이질성으로 인해 조직 구성원들이 느끼는 기술적 이질감은 더욱더 증가할 수밖에 없다. 이로 인해 조직원들은 정보보안에 대해 불편함을 느끼거나, 자신의 업무의 생산성을 저해한다고 느끼게 된다. 또한 기존의 정보기술 이외에 또 다른 기술인 보안 시스템에 대한 적응과 학습이 필요하기 때문에 조직원들이 느끼는 보안 스트레스는 자연스럽게 증가할 수밖에 없다. 예를 들어 복잡한 시스템 인증 절차나 다양한 정보보안 정책의 준수는 조직 구성원들에게 또 다른 부담으로 작용할 수 있다. 이처럼 보안도 기술과 무관하지 않고 다양한 스트레스를 유발할 수 있는 자극제로 작용함에도 불구하고 관련 연구는 매우 부족하다.

기존 연구들은 정보보안 사고의 빈도, 사고로 인한 손실을 예방하고 감소하는 것 등으로 정보보안 성과를 측정하는 방법과 종합적으로 평가할 수 있는 접근 방법이 주를 이루었다. 하지만, 정보보안 성과에만 치중하다보면 정보보안이 강화되고 정보보안 통제가 이루어질 수밖에 없다. 이에 따라 조직 구성원들이 업무에서 느끼는 불편함은 간과될 수 있다. 정보보안의 중요성은 당연히 인정하지만, 이로 인한 구성원들의 보안 스트레스는 점점 증가하고 있으며, 어떤 요인들로 인해 보안 스트레스가 증가하고 있는지 대한 연구는 미흡하다.

특히 본 연구는 조직 구성원을 ICT보안 업무 종사자와 일반 사무직

종사자로 구분하여 연구하고자 한다. 보안시스템을 도입하고 정책을 수립하는 ICT보안 업무 종사자와 그 시스템을 사용하고 정책을 따르는 일반 사무직 종사자로 구분하여 각각이 느끼는 보안 스트레스와 그 차이를 분석하고자 한다. 또한, 회사 내 직위 즉 일반 직원과 간부 간에 느끼는 보안 스트레스에 차이가 있는지를 분석하고자 한다. 노동조합에 속해 있는 일반 직원과 일반직원들의 관리자 역할을 맡고 있을 뿐만 아니라, 노동조합에 속하지 않고 회사 간부로 속해 있는 3직급 이상의 직원들이 느끼는 보안 스트레스를 비교하여 그 차이를 분석하고자 한다.

본 연구를 통해 ICT보안 업무 종사자는 정보보안 기술이나 솔루션을 새롭게 개발할 수 있는 능력보다는 기존의 정보보안 기술이나 솔루션에 대한 기본적인 이해를 통해 조직 구성원들에게 친화적인 보안 업무가 이루어질 수 있도록 노력하기 바란다. 보안 업무 종사자들은 정보보안을 위하여 이러한 기술들을 실제 ICT시스템에서 어떻게 활용할 수 있으며, 이러한 기술들이 제공하는 정보보안 기능의 범위와 한계가 무엇인지를 제대로 이해하고, 일반 사무직 종사자가 쉽게 이해할 수 있도록 설명할 수 있어야 한다. 정보보안 기술로 해결할 수 없는 부분을 보완하기 위하여 어떠한 관리적인 대책이 추가되어야 할 것인지에 대해 지속적으로 고민해야한다. 위에서 일방적으로 지시하는 형태의 보안 정책은 할 수 없이 수행하는 귀찮은 업무로 생각하기 쉽다. 정보보안이 왜 필요하고 이것이 적절히 이루어지지 못할 때 어떠한 피해가 돌아오게 될 것인가 등에 대한 설명이 있어야 하고 이에 대한 홍보와 교육이 뒤따라야 한다. 정보보안을 관리하고 있는 ICT보안 업무 부서에서는 정보보안 업무를 일방적인 지시와 규정에 따라 관련 부서에서 요구하는 대로 타 부서 및 관련 업무 종사자가 수행해야 한다는 일방적인 사고방식을 버려야 한다. 이러한 방식은 정보보안에 대한 인식의 부족을 초래하여 형식적인 정보

보안 업무에 그치게 되기 쉽고, 자칫 잘못하면 조직 구성원에게 보안 스트레스를 증가시킬 수 있다.

제 2 절 연구 방법

연구목적을 달성하기 위하여 먼저 정보보안의 개념과 그에 따라 발생하는 통제와 스트레스에 대한 문헌적 고찰을 진행하였고, 이를 토대로 K공사 구성원들의 정보보안 스트레스 수준을 실증적으로 분석하였다.

본 연구의 실증 분석에서는 K공사 본사 및 전국 각지의 사업소를 대상으로 실증적 분석을 실시했으며, 대상 사업소의 범위는 1차사업소 및 3급 이상 2차 사업소로 한정했다. 왜냐하면 지역 서비스센터 등 3급 이하 사업소는 사업소장을 제외한 조직구조가 수평조직에 가깝고 조직구성원 측면에서도 해당지역 출신 인사가 많이 배치되어 있는 등 일반적인 공기업 조직의 특성과 많이 다르기 때문이다. 따라서 사업본부 및 3급 이상의 사업소로 분석대상을 제한함으로써 연구의 효율성을 기하였다. 연구 대상 조직 및 인원은 본사 및 3개 사업본부 25개 팀 300명을 표본 대상으로 하여 설문조사를 시행하였다. 설문지 조사는 입사 6개월 이상인 직원을 대상으로 설문지를 배포하여 통계분석을 실시하였다. 설문기간은 2013년 2월 18일 ~ 2월 27일까지 실시하였다.

설문지는 여러 선행연구 설문지를 발췌·보완하여 사용하였으며, 설문항목은 정보보안 스트레스에 유의미한 영향을 준다고 알려진 요소들 즉 보안관심도, 회사 보안 전략 신뢰도, 회사 보안 교육수준, 근무분야, 직위, 근무지를 독립변수로 정하고 종속변수로는 기술적, 물리적, 관리적 정보보안 스트레스를 정하여 관련된 총 32개 문항을 5단계 척도로 구분

하였다. 또한 정보보안 교육이 정보보안 스트레스에 미치는 영향을 분석하기 위해 그 교육시간에 대한 서술형 조사문항을 포함하여 분석하였다.

실증분석 절차로는 연구모형의 설계와 함께 연구가설을 설정하였으며, 측정도구의 신뢰성과 타당성을 확보한 후에 가설검증을 실시하였다. 본 연구의 가설을 실증적으로 분석하기 위하여 회수된 설문지 자료에 대한 부호화(Coding) 과정을 수행하고 SPSS 통계 패키지를 이용하여 연구가설에 대한 다중회귀분석을 시행하였다.

제 2 장 이론적 논의 및 선행연구 검토

제 1 절 정보보안에 관한 선행연구 고찰

1. 정보보안의 개념

우리가 흔히 사용하는 정보화시대, 정보의 홍수 등 정보가 들어가는 말은 흔한 일이 되어 버렸다. 아침에 일어나면 뉴스를 통해 기상정보를 듣고, 출근하면서 교통정보를 접하며, 회사에서는 마케팅 정보를 가지고 계획을 실행에 옮긴다. 일과 후에는 증권정보를 통해 투자한 증권의 가격 상승과 판매 시점에 대해 알아보고, 피곤해지는 저녁 무렵이면 건강에 관련된 정보를 인터넷이나 책 또는 다른 매체들을 통하여 접하고 있다. 이처럼 정보는 우리 주변을 구성하고 있는 의미 있는 사실 자료들이다. 국가정보화 기본법(2011)에 의하면 정보란 “특정 목적을 위하여 광(光) 또는 전자적 방식으로 처리되어 부호, 문자, 음성, 음향 및 영상 등

으로 표현된 모든 종류의 자료 또는 지식”을 말한다. 공공기관의 정보공개에 관한 법률(2013)에 의하면 정보란 “공공기관이 직무상 작성 또는 취득하여 관리하고 있는 문서(전자문서 포함)·도면·사진·필름·테이프·슬라이드 및 그 밖에 이에 준하는 매체 등에 기록된 사항”을 말한다. 결국 정보는 어떠한 목적을 가지고 생성되는 것이기 때문에 그 정보의 내용을 알아야 하는 사람이 있고, 알아서는 안 될 사람으로부터는 보호되어야 한다는 보안이라는 측면을 내포하고 있다. 이는 정당한 사용자가 필요한 정보를 알 필요성과 인가되지 않은 자는 그 정보에 접근할 수 없게 보호되어야 한다는 당위성에 기초한 의미를 말하는 것으로 진정한 정보사회의 성패는 바로 이 정보보안의 문제에서 비롯된다고 할 수 있다. 특히 정보보안은 기업의 중요 정보자산에 대한 보호가 그 주목적이며, 정보자산은 유·무형의 기업 내 모든 정보관련 자산을 의미한다. 아래의 <표 2-1>은 기업 내 정보보안 체계에 의해 보호가 되어야 하는 정보자산에 대한 분류 정보이다.(구자면, 2012)

이렇듯 비인가된 상황으로부터 정보는 보호되어져야 한다는 당위성에 기초한 개념은 정보보안(Information Security), 정보보호(Information Protection)로 혼용되어서 사용되고 있다. 본 연구에서 사용할 정보보안과 정보보호에 대한 의미를 살펴보면 정보보호는 일반적으로 정보보안이라고도 하는데, 정보보안은 주로 정보통신망 등 기술적 측면에서의 정보보호로 협의의 정보보호이며, 오늘날에는 기술적 측면뿐 아니라 관리적, 제도적 차원을 포괄하는 광의의 정보보호로 이해되고 있다. 국외 연구에서는 정보보안 관련 연구에서 보호(Protection)이라는 용어를 사용하지 않고, 보안(Security)이라는 용어를 주로 사용한다. 하지만 국내 연구에서는 정보보호와 정보보안의 용어가 혼용되어서 사용되고 있으며, Security라는 용어를 대부분 정보보호의 의미로 사용하고 있다.

<표 2-1> 정보자산의 분류

구분	세 부 내 용
정 보	• 기업이 보유 및 관리하고 있는 모든 종류의 정보 • R&D 정보, 영업정보, 조직정보, 임직원 정보 등
문 서	• 기업이 보유 및 관리하고 있는 모든 문서(전자, 출력) • 정책/지침, 업무관련 문서, 인사기록, 송장 등
인 력	• 기업과 관련 있는 모든 인원 • 내부직원, 퇴직자, 협력업체, 고객 등
소프트웨어	• ICT 시스템에 사용되는 프로그램 • 운영시스템, 어플리케이션 프로그램, 통신 프로그램 등
설 비	• 업무에 사용되는 하드웨어 • 업무용 서버, 네트워크 장비, PC, 책상, 캐비넷 등
기 타	• 외부기관으로부터 제공받는 서비스 • 정보서비스, 통신서비스 등

Solms(1998)는 정보보안 영역에서는 보호되어야 하는 정보의 속성을 비인가된 노출로부터 보호하는 기밀성(confidentiality), 비인가된 변조로부터 보호하는 무결성(integrity), 적시에 인가된 사용자에게 정보를 제공하는 가용성(availability)으로 정의하였다. 정보의 기밀성, 무결성, 가용성을 해칠 수 있는 잠재 요인을 위협(threat)이라 하고, 위협에 의하여 침해되는 정보 또는 정보 자산의 속성을 취약성(vulnerability)이라 하였다.

신영진(2004)은 정보보안을 정보의 보전, 정보보호는 정보의 보장의 의미로 구분하고 있다. 즉, 정보보안은 정보의 가치가 상실되지 않도록

보호하기 위한 제반 수단 및 대책을 강구하기 위한 행위이며, 정보보호는 정보의 정상적 유지를 위해 물리적, 기술적, 자연적 장애기능을 사전예방 및 사후 회복조치 하도록 하는 것을 말한다. 또한, 정보화촉진기본법 제2조 정의에서 “정보보호라 함은 정보의 수집, 가공, 저장, 검색, 송신, 수신 중에 정보의 훼손, 변조, 유출 등을 방지하기 위한 관리적, 기술적 수단을 강구하는 것을 말한다.”고 언급하고 있다. 다시 말하면 정보보호란 자신 또는 정보자의 자산을 내/외부의 불법적 행위(해킹, 크래킹)나 천재지변 등의 사고로부터 보호하는 모든 과정이나 행위라고 정의하고 있다.

이선중・이미정(2008)에 의하면 정보보호는 대개 물리적・기술적 차원, 행정・관리적 차원, 사회・윤리적 차원으로 구분되며, 최근 들어 기술적 측면에서 점차 관리, 제도적 측면을 포함하는 광의의 개념으로 정의된다. 이에 따라 정보보호는 컴퓨터, 유・무선 네트워크를 기반으로 하는 정보시스템에서의 정보에 대한 온・오프라인 상 접근, 훼손, 변조, 유출 등을 방지하고, 행정정보 및 개인정보 등 데이터, 정보시스템, 콘텐츠 및 서비스 등을 보호하는 사전예방 및 사후처리 활동을 하는 제반의 기술적, 관리적, 제도적 조치로 재정의할 수 있다. 이는 기술적 측면의 정보보안을 기반으로, 관리 및 제도적 활동으로의 성숙을 강조한 것이다.

이렇듯 다소 혼용되어 사용되고 있는 정보보안과 정보보호의 개념을 정리하자면 정보보안(Information Security)은 자산이 되는 정보의 완전성을 지키는 것이 주가 되는 수단적 개념으로, 정보의 안정성(Safety)과 무결성(Integrity)의 보전을 추구하는 의미로써 사용되고 있다. 이에 반해서 정보보호(Information Protection)는 그 관점을 정보가 아닌 외부의 위협에 두고, 사고를 예방하고 사후회복에 중점을 두는 개념이다. 정보보호는 내부의 정보가 외부에 유출되거나 침해되는 것을 막는 것에 중점을

둔다. 상술된 두 가지 개념을 비교해 볼 때에 정보보호의 개념이 정보보안을 포함한 포괄적인 개념이라 볼 수 있다. 정보보안과 정보보호를 비교해 보면 <표 2-2>와 같다.(강성민 등 2008; 김영곤 2010)

<표 2-2> 정보보안과 정보보호

구분	정보보안	정보보호
적용	ICT 시스템 보안, 해킹방지 암호설정, 인증	국가정보보호, 개인정보보호, 기업단체 정보보호
성격	완전성(안전성, 무결성) 보전	비밀성 보장
정의	정보의 가치가 상실되지 않도록 보호하기 위한 제반 수단과 대책을 강구하기 위한 행위	정보의 정상적인 유지를 위해 물리적, 기술적, 자연적인 장애기능을 사전 예방, 사후 회복 조치

그러나, 정보보안 및 정보보호는 'Security'라는 용어에 기반을 두고 있으며, 기밀성(confidentiality), 무결성(integrity), 가용성(availability)을 확보하는 것에 동일한 목표를 두고 있으므로, 본질적으로 동일한 용어로 생각할 수 있다. 다만, 연구자들이 'Security' 용어를 보안 또는 보호로 양분하여 해석함으로써 두 가지 용어가 생겨나게 되었고, 이후에 동일한 개념을 각 연구자가 혼용하여 사용함으로써 현재의 개념적 혼란이 있었던 것이다. 본 연구에서는 정보보안기술 사용과 관련하여 내적인 정보의 완전성과 외부의 보안 위협 침해를 모두 고려함으로써 두 용어의 의미를 모두 필요로 한다. 따라서 본 연구에서는 두 용어를 포괄하는 개념으로서의 정보보안(Information Security)의 용어를 사용한다.

2. 정보보안의 범위

일반적으로 전통적인 정보보안의 분류는 인원보안, 시설보안, 문서보안, 통신보안, 시설보안으로 구분하고 있으나, 정보통신기술의 발전, 정보공유와 지식관리 등 정보화 영역의 확장 및 관련 업무 세분화에 따라 보안 분야도 다양하게 변화되고 있다.

김현수・정해철(1999)은 정보보안의 여러 측면을 고려하여 수준을 판단하는 기준으로 기업 또는 국가의 정보보안 수준을 측정하고 정보보안 전략 및 정책 수립에 활용될 수 있는 정보보안 지표의 개념을 정의하였다. 비교적 오래 전부터 국내에서 연구된 정보화 지표의 경우와 같이, 정보보안 지표는 정보보안의 각 부문에 대해 수치화된 자료를 이용하여 평가하고, 이를 종합적으로 점수화하여 나타낸 수치라고 정의하였다. 정보보안 분야를 물리적 보안, 기술적 보안, 관리적 보안, 정보보안 환경 등 4개 분야로 나누고 각 분야별 세부항목을 <표 2-3>과 같이 제시하였다.

남길현・원동호(2010)는 정보보안 분야별 요소들을 기술적, 물리적, 관리적 보안으로 제시하였다. 첫째, 기술적 보안은 정보 시스템, 통신망, 정보(데이터)를 보호하기 위한 가장 기본적인 정보보안 통제 대책으로서 정보보호 제품을 사용하여 정보 시스템에 대한 접근 통제, 저장된 데이터나 송신 및 수신 중에 데이터를 은폐하는 암호 기술적용, 재난 복구를 대비하기 위한 백업 체제, 정보 시스템 자체에 보안성이 강화된 시스템 소프트웨어를 사용하는 등의 대책이 기술적 보안에 속한다. 둘째, 물리적 보안은 화재, 수해, 지진, 태풍 등과 같은 자연재해로부터 정보 시스템이 위치한 정보처리시설을 보호하기 위한 자연 재해대책과 조직내부 불순세력이나 적의 파괴로부터 정보 시스템을 보호하기 위한 출입통제, 시건장치 등의 물리적 보안 통제로 구분된다. 셋째, 관리적 보안은 법・제

<표 2-3> 정보보안 요소 항목의 계층적 구조

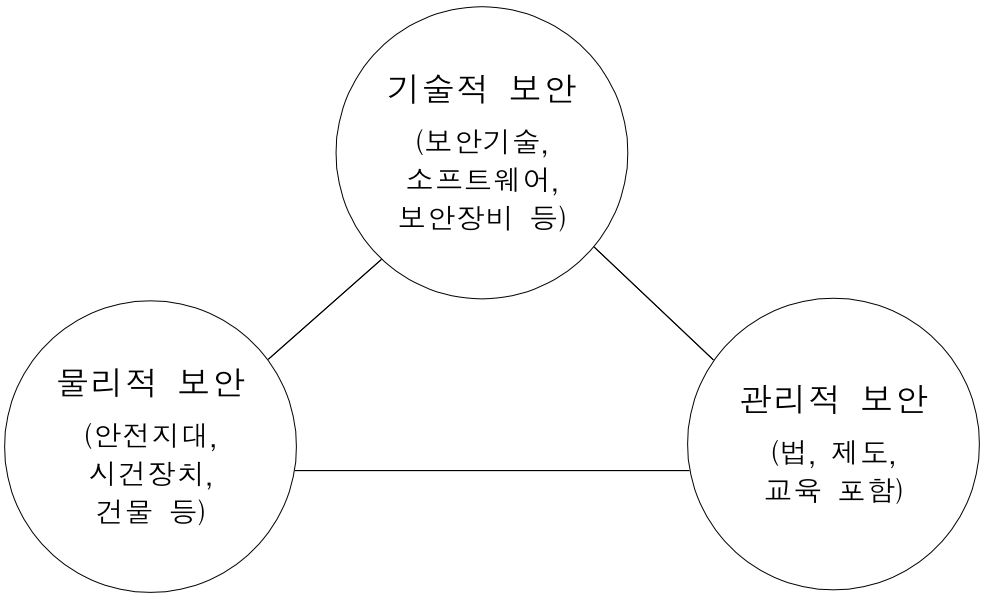
대분류	중분류 (소항목)
물리적 보안	물리적 접근 통제(14), 환경 위험에 대한 대책(5), 업무 계속성 확보 계획(3)
기술적 보안	시스템 접근 통제(4), 감사추적(3) 응용 프로그램 보안(7), 데이터베이스 보안(2) 하드웨어 보안(2), 네트워크 보안(6) PC 및 바이러스 보안(3)
관리적 보안	보안 조직(7), 보안정책(2), 보안계획(2), 자산파악(2), 위험분석(2), 인사보안(3), 유지보수 점검(3)
정보보안 환경	정보보안 의식(3), 정보보안관련 투자(2), 정보보안 법/제도/표준(2), 보안상태 점검목록 및 수행(4)

도・규정・교육 등을 확립하고, 보안계획을 수립하고 이를 운용(보안 등급, 액세스 권한 등)하며, 위험분석 및 보안감사를 시행하여 정보시스템의 안전성과 신뢰성을 확보하기 위한 대책이다. 조직체의 정보보안을 효과적으로 보장하기 위해서는 다양한 기술적인 보호대책 뿐만 아니라 이들을 계획하고, 설계하며 관리하기 위한 제도, 정책 및 절차 등의 관리적 통제 대책도 매우 중요하다.

지금까지 살펴본 바로 정보보안이란 일반적으로 공공분야의 비밀 또는 기밀이 고의 또는 과실로 인한 누설로부터 관련기관 및 조직 등에 초래할 수 있는 제반 피해를 예방하거나 최소화 한다는 의미에서 정보보호의 한 유형이라고 불 수 있다. 일반적으로 정보보안은 기술적 측면에 따른 대응책에 초점을 둔 반면, 정보보호는 기술적 대응을 포함한 다양한 정보보호의 정책적 대응방안을 포함하므로 그 범위가 넓다고 볼 수 있

다. 본 연구에서는 정보보안에 대한 이론 및 선행연구들을 고찰하여 정보보안 요소를 <그림 2-1>과 같이 구분하고, 정보보안을 기술적, 물리적 및 관리적 측면까지 포함하는 광의의 개념으로 정의하였다.

<그림 2-1> 정보보안 분야



3. 정보보안 현황

우리나라는 국외에서 발표되는 지수들을 보더라도 인터넷 강국으로서의 면모를 유감없이 발휘하고 있다. 2012년 발표자료 기준인 <표 2-4>를 살펴보면 우리나라는 UN(국제연합, United Nations)의 전자정부 발전지수와 온라인 참여지수 1위, ITU(국제전기통신연합, International Telecommunication Union)의 ICT 발전지수 1위를 차지하는 등 주요 정보통신지수에서 최고 수준을 나타내고 있다.

한편 우리나라의 인터넷 이용 현황을 살펴보면, 2012년 인터넷 이용자가 3,812만명(인터넷이용률 78.4%)에 이르고 있다. 10대와 20대의 99.9%, 30대의 99.5%가 인터넷을 이용하고 있고, 어린이(3~9세)는 88.2%, 40대는 89.6%의 인터넷 이용률을 보이고 있다.

이에 따라 인터넷을 이용한 각종 서비스의 이용도 보편화되고 있다. 인터넷뱅킹 등록자 수는 꾸준히 증가하여 2012년 8,000만명을 돌파하였다. 2012년 전자상거래 총 거래액은 1,144조 6,890억원으로 나타나 드디어 1,000조원 규모를 돌파하였다.

<표 2-4> 우리나라 주요 정보통신지수 순위

[작성기관] 지수명	목적/성격	지수특징	우리나라순위 (조사대상 국가 수)					최근 발표일
			'08	'09	'10	'11	'12	
[UN] 전자정부 발전지수	국가별 전자정부 수준 측정	▪ 온라인서비스, 정보통신 인적자본 부문 지수로 구성 ▪ 격년 주기로 발표	6	-	1	-	1 (193)	'12년 2월
[UN] 온라인 참여지수	국가별 온라인을 통한 시민참여 정도 측정	▪ 전자정보, 전자컨설팅, 전자의사결정 등 3개 부문 ▪ 격년 주기로 발표	2	-	1	-	1 (193)	'12년 2월
[ITU] ICT 발전지수	국가별 정보사회의 발전정도 및 정보격차를 측정	▪ ICT 접근성, 이용, 활용능력 등 3개 부문	-	2	3	1	1 (155)	'12년 10월
[WEF] 네트워크 준비지수	국가별 개인, 기업, 정부 IT의 환경, 준비도, 활용도 측정	▪ IT를 위한 제반 환경, IT의 수혜를 누릴 수 있는 준비도, 최신 ICT의 활용도, ICT발전의 경제적·사회적 영향 등 4개 부문	9	11	15	10	12 (142)	'12년 4월

[출처 : 한국정보화진흥원, 국제 정보화지수 현황, 2012.9]

하지만, 이처럼 정보화 사회의 진전에 따라 역기능도 확대되고 있다. 악성 댓글, 스팸메일, 개인정보 유출, 금전적인 목적을 대상으로 하는 피싱(Phishing)이나 파밍(Pharming)에 따른 개인적인 피해가 증가하고 있으며, 불건전 정보 유통, 개인 사생활 침해 등과 같은 부작용이 심각한 사회문제로 대두되고 있다. 또한 네트워크의 보급 확대에 따른 정보교환 및 공유로 인하여 정보에 대한 불법적인 접근에 의한 주요 기밀의 유출 가능성도 높아지고 있다.

이러한 문제점은 계속 새로운 수법이 등장하면서 대처를 더욱 어렵게 하고 있다. APT(지능형 지속위협, Advanced Persistent Threat)는 대규모의 피해를 발생시키고 있으며, 피싱은 오늘날 스미싱(Smishing)이라는 새로운 형태로 변화하면서 더욱 수법이 교묘해지고 있다.

2011년 한 해 동안 한국인터넷진흥원에서 접수·처리한 침해사고 통계를 분석해 본 결과 <표 2-5>에서 보여지는 것처럼 악성코드 피해신고 건수는 총 21,751건으로 전년도 대비 21.3% 증가하였으나, 해킹사고 접수처리 건수는 11,690건으로 전년도 대비 28.3% 감소한 것으로 나타났다.

2011년에는 다양한 악성코드 신종 및 변종이 출현하여 많은 피해를 발생시켰다. 특히 3.4 DDoS[2] 및 금융기관 해킹사고 등 악성코드로 인한 대규모 인터넷 침해사고가 발생하였고, 안드로이드 스마트폰을 대상으로 하는 악성코드가 급증한 한 해였다.

이러한 정보화의 역기능은 사회 혼란을 야기하고 국가안보에 악영향을 미칠 가능성이 있기 때문에 심각한 문제가 될 수 있다. 오늘날 국가기관, 정당, 언론사 등을 겨냥한 정치적 목적의 사이버 공격이 더 이상

2) DDoS(Distributed Denial of Service) : 일반적으로 악성코드나 이메일 등을 통하여 일반 사용자의 PC를 감염시켜 이른바 '좀비PC'로 만든 다음 동시에 '서비스 거부 공격(Denial of Service attack ; DoS)을 함으로써 시스템이 더 이상 정상적 서비스를 제공할 수 없도록 만드는 것을 말한다.

낯선 일이 아니다. 또한 일상생활에서 ICT에 대한 의존도가 높아지고, 주요 기반시설이 정보통신 네트워크에 의해 관리·통제됨에 따라 해킹 등의 공격행위로 주요 기반 시설에 커다란 위협을 가할 수 있게 되었다. 따라서 정보보안이 중요한 문제임을 깊이 인식할 필요가 있다.

<표 2-5> 2011년 침해사고 접수처리 건수 (단위: 건)

구분	2010년 합계	2011년				2011년 합계
		1/4분기	2/4분기	3/4분기	4/4분기	
악성코드 피해신고	17,930	6,333	5,884	5,331	4,203	21,751
해킹사고 접수처리	16,295	2,881	3,017	2,968	2,824	11,690
- 스팸릴레이	5,216	838	1,344	647	898	3,727
- 피싱 경유지	891	93	75	106	91	365
- 단순침입시도	4,126	825	714	710	712	2,961
- 홈페이지변조	3,043	373	362	749	370	1,854
- 기타해킹	3,019	752	522	756	753	2,783

※ 스팸릴레이 : 보안이 취약한 시스템이 스팸발송에 악용된 건 수

※ 피싱 경유지 : 보안이 취약한 국내 시스템이 주로 해외 기관의 사칭사이트로 악용된 건 수

※ 단순침입시도 : 인터넷에 연결된 시스템의 취약점을 찾기 위하여 네트워크 서비스를 파악해 보는 공격 건 수

※ 폼페이지변조 : 해커에 의해 홈페이지 화면이 변조된 홈페이지 탐지 건 수

[출처 : 한국인터넷진흥원, 인터넷 침해사고 동향 및 분석월보, 2011.12]

제 2 절 정보보안 통제에 관한 선행연구 고찰

그동안 정보보안에 대한 연구는 외부의 공격으로부터 내부의 정보자

원을 안전하게 지키고자 하는 요인에 집중되어 왔다. 그러나 정보화 역기능에 대응하기 위해서는 침입차단 시스템(Firewall)[3], 침입탐지 시스템(IDS:Intrusion Detection System) 및 침입방지 시스템(IPS:Intrusion Prevention System), 웹 방화벽(WAF:Web Application Firewall) 등 다양한 정보보안 솔루션과 함께 관리 속성으로 다양한 통제요인이 함께 적용되어야 기대 이상의 효과를 올릴 수 있다. 그러다보니 현재 운영되고 있는 대부분의 정보보안 활동이 외부 공격자에 대비한 방어 위주의 시스템 보안에만 치중되어 있다. 하지만 정작 중요한 것은 권한을 가진 관리 내부자에 의하여 발생하는 자료 유출에 대해서 소홀하게 대처하고 있다는데 문제가 있다. 여기에서부터, 조직 내부의 위험 요소를 줄이기 위한 정보보안 통제의 개념이 등장한다.

정보보안 통제는 보안 사고를 미연에 방지하거나 발생된 보안사고의 영향을 최소화하기 위한 기술적, 관리적 활동을 의미하는 것으로(Wack & Carnahan, 1989), 적절한 보안통제가 이루어지지 않을 경우 보안 운영 절차, 기술적 통제 및 물리적 통제 등의 미비나 결여로 인하여 정보시스템이 취약성을 가지게 되며, 생성된 취약성은 특정 위협에 ICT시스템을 노출시켜 위험을 초래하게끔 한다.

특히, 조직 내부에서 증가하는 보안 위협을 효율적으로 관리하기 위해서는 조직 구성원의 통제가 불가피하다. 정보보안 활동이 효과적으로 이루어지기 위해서는 위험 분석 활동을 통하여 도출된 위험에 적절하게 대응할 수 있는 정보보안 통제가 구현되어 있어야 한다. 즉, 정보보안 활동은 적절한 정보보안 통제의 구현이 이루어질 때 정보보안 성과에 더욱 영향을 미칠 수 있다. 반대로 구현된 정보보안 통제는 정보보안 활동이

3) 침입차단 시스템(Firewall) : 인터넷에 인터넷 프로토콜(IP)로 접속되어 있는 네트워크를 불법적인 침입으로부터 보호하기 위하여 게이트웨이에 설치되는 접속 제한 시스템. 방화벽이라고도 한다.

적절히 이루어질 때만이 정보보안 성과에 의도된 효과를 미칠 수 있다. 예를 들어, 구현된 정보보안 통제가 제때에 유지 보수되지 않거나 지속적인 모니터링이 이루어지지 않는다면 구현된 정보보안 통제는 실질적 효과가 없는 형식적 통제에 지나지 않게 된다.

정보보안 통제에 관한 국제 표준으로서 기업의 정보보안 관리의 기준선 통제를 제안한 ISO 17799(Information Security Management Systems, 2000)에는 다음 <표 2-6>과 같이 기술, 관리 및 물리분야의 총 10개 통제 분야가 있다.

<표 2-6> ISO 17799의 정보보안 통제

통제 분야	정 의
정보보안 정책	정보보호에 대한 경영자의 지침과 지원을 위한 통제
조직적 정보보안	조직 내의 정보보안 관리를 위한 조직, 제3자, 외주 조직 통제
자산 분류와 통제	조직 자산의 적절한 보호를 위한 자산 분류와 관리 통제
인적보안	설비의 사람에 의한 오류, 절도, 사기 및 오용의 위험을 감소하기 위한 통제
물리적 및 환경적 보안	업무 영역 및 정보에 대한 비인가된 물리적 접근, 손실 그리고 간섭을 예방하기 위한 통제
전산기 및 네트워크 관리	정보처리 설비의 정확하고 안전한 운영을 확인하기 위한 통제
시스템 접근 통제	정보에 대한 접근을 제한하기 위한 통제
시스템 개발 및 유지보수	정보시스템에 정보보안이 구현되었음을 확인하기 위한 통제
업무 연속성 계획	업무 활동의 방해에 대응하고, 중요 오류 및 재난에 의한 영향으로부터 핵심 업무 프로세스를 보호하기 위한 통제
준수	민형사법, 규정, 계약사항 및 정보보호 요구사항의 위반을 방지하기 위한 통제

국내 표준으로는 한국인터넷진흥원(KISA:Korea Internet and Security Agency)에서 운영하는 ISMS(Information Security Management Systems) 인증 제도가 있다. ISMS는 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제47조를 근거로 한국인터넷진흥원이 정보통신 서비스제공자, 정보통신 서비스를 위해 물리적 시설을 제공하는 자, 민간사업자 등 인증대상기관이 수립·운영하고 있는 ISMS의 기술, 물리, 관리적 정보보안 대책이 인증심사기준에 적합한지를 평가하여 인증하는 제도이다. 5단계 관리과정에 따라 정보보호 위험을 평가하여 15개 분야 120개 통제항목 중에서 필요한 통제를 선정, 구축하고 문서화하여 운영하고 사후관리 할 것을 요구한다. 5단계의 관리과정은 ①정보보안 정책 수립 ②정보보안 관리체계 범위 설정 ③위험관리 ④구현 ⑤사후 관리의 과정을 거쳐 수립·운영된다. ISMS는 정보보안에 관련된 위험을 통제하기 위한 대책을 수립하고 관리하는 체계라고 할 수 있고, 인증심사 기준에서는 15개 통제 분야에 대해 120개 세부 통제사항을 제시하고 있으며, 아래 <표 2-7>와 같이 분류된다.

<표 2-7> ISMS 인증 통제 분야

통제 분야	세부 통제사항	항목수
정보보안 정책	정책의 승인 및 공표, 체계, 유지 관리	5
정보보호 조직	조직의 체계 및 책임과 역할	4
외부자 보안	계약 및 서비스 수준협약 등	4
정보자산 분류	정보자산의 조사 및 책임할당, 정보자산의 분류 및 취급	4
정보보안 교육 및 훈련	교육 및 훈련프로그램 수립, 교육 훈련의 시행 및 평가	4

인적보안	책임할당 및 규정화, 직원의 적격 심사, 주요 직무 담당자 관리, 비밀 유지	5
물리적 보안	물리적 보호구역, 물리적 접근통제, 데이터 센터 보안, 장비보호, 사무실 보호 등	12
시스템 개발 보안	분석 및 설계, 구현 및 이행, 변경 관리	13
암호통제	암호정책, 암호사용, 키관리	3
접근통제	접근통제 정책, 사용자 접근관리, 접근통제 영역 등	14
운영관리	운영절차와 책임, 시스템/네트워크 운영관리, 악성소프웨어 통제 등	22
전자거래 보안	교환합의서, 전자거래, 전자우편, 공개서버의 보안관리, 이용자 공지사항	5
보안사고 관리	대응계획 및 체계, 대응 및 복구	7
검토 모니터링 및 감사	법적 요구사항 준수 검토, 정보보호 정책 및 대책 준수 검토, 모니터링, 보안감사	11
업무 연속성 관리	업무연속성 계획 수립과 구현, 시험, 유지관리	7

홍기향(2003)은 정보보안 활동과 통제가 정보보안 성과에 미치는 영향을 분석하였다. 정보보안 통제는 정보보안 성과에 직접적 영향을 미치지 않으나, 정보보안 활동이 정보보안 성과에 영향을 미치는 과정에서 이를 조절하는 기능이 있음이 나타났다. 즉, 정보보안 활동의 수행 과정에서 적절한 정보보안 통제가 채택되어 구현됨으로써 정보보안 성과를 더욱 높일 수 있다는 것이다. 따라서 조직의 정보보안 관리에 있어 정보보안 활동이 일정 수준에 도달 한 조직에서는 정보보안 활동의 성과를 더욱 향상시키기 위해서는 적절한 정보보안 통제를 도입하는 방향으로 성과의 향상을 유도할 수 있을 것으로 판단되었다. 또한 조직의 정보관리 연혁이 오래되어 정보관리 활동의 일부로 정보보안 활동이 수행된 조직이 보다 가시적인 정보보안 성과를 창출하기 위해서는 기존의 정보보

안 관리 활동을 적절한 정보보안 통제의 도입과 함께 체계화할 필요가 있다는 근거를 제공하였다.

김종기 등(2006)의 연구에서는 컴퓨터 바이러스 통제의 효과성에 영향을 미치는 요인을 정보보안 통제 및 사용자 특성으로 보고, 또 이 두 요인의 선행요인으로 조직의 보안정책을 설정하여 모형화하고 실증분석을 수행하였다. 분석 결과, 먼저 조직의 정보시스템 사용기준을 제시한 보안정책이 보안통제에 미치는 영향은 유의한 것으로 나타났다. 이는 조직의 보안정책이 명확하게 수립되어 있을 경우 컴퓨터 바이러스의 대응을 위한 적절한 관리활동이 가능해질 수 있음을 의미하는 것으로 보안정책은 조직의 체계적이고 종합적인 정보보안 활동 수행의 전제조건이라는 점을 시사한다. 또한 조직의 정보보안 통제와 보안효과 사이의 관계 또한 통계적으로 유의하게 나타났다. 이는 정보보안을 위한 보안절차, 기술 및 관리적 활동이 원활할 경우 컴퓨터 바이러스에 의해 발생하는 감염의 확산을 방지하거나 감염피해를 축소할 수 있으므로 보안효과를 기대할 수 있다는 것으로 해석할 수 있다. 역으로 조직의 보안관리 활동이 부적절할 경우 정보시스템이 취약성을 가지게 되므로 컴퓨터 바이러스에 의한 공격의 목표가 되고, 이에 따라 보안효과는 낮아지게 된다는 것이다.

박준형(2007)은 억제이론을 근거로 하여 인간의 행위에 제약을 주는 요소로 인간의 두려움을 근간으로 하는 처벌과 인간의 자기 통제능력에 대한 믿음을 근간으로 하는 적절한 교육 즉 윤리가 보안침해사고를 일으키는 조직 구성원의 인식에 어떤 영향을 미치는지에 대해 실증 분석하였다. 그 결과 정보보안에 대한 처벌과 윤리적 억제에 대한 인식이 정보보안 효과에 긍정적 영향을 주는 요인임을 알 수 있었고, 조직 구조와 규모, 유형의 차이에 따라 처벌과 윤리적 교육에 대한 구성원의 인식 차가 존재함을 밝혀냈다. 즉, 각각의 구성원들은 각자의 개인적 성향이 분명히

존재하지만, 정보보안과 관련된 조직 내 일상 업무에 있어서 조직의 특성과 업무 유형에 따라 처벌과 윤리적 교육에 대한 인식이 차이가 있음을 의미하는 것이다.

백민정(2010)은 조직의 정보윤리평가/통제, 정보윤리정책, 정보윤리교육제도 등이 정보보안인식에 영향을 미치는 것으로 분석하였다. 이는 조직의 정보보안에 대한 활동을 조직 구성원들이 인식하고 있을 때 조직 구성원들은 정보보안 인식의 수준이 높아질 수 있다는 것을 나타낸다. 따라서 조직 구성원들의 정보보안 인식 제고를 위해서는 통제에 대한 명확한 설명 등을 통한 조직 차원의 다양한 지원이 필요하다.

정구헌・정승렬(2011)은 조직 내부에서 증가하는 보안 위협을 효율적으로 관리하고 통제하기 위해서는 주로 사용하는 바이러스 예방 프로그램이나 침입통제 같은 기술적 측면에만 의존해 여전히 정보유출의 가능성을 남겨두는 현실을 고려할 때, 이를 보완하기 위해서는 보안 위협에 대한 개인행동이나 보안 기술을 사용하는 조직 구성원에 대한 물리적 통제와 관리적 통제가 병행되어야 한다고 하였다.

즉, 안전하게 내부 조직의 정보와 시스템을 보호하기 위해서는 기술적인 측면보다 관리적 측면과 물리적 측면에서 효과적인 보안 정책을 세우고 이를 조직 구성원들이 실행할 수 있는 속성을 규명하여 자사에 맞게 동기부여를 하는 것이 매우 중요하다고 강조하였다.(이창환 2011; 송영미 2013)

박철주・임명성(2012)은 정보보안이라는 하나의 목표를 달성하기 위해서는 새로운 정보보안 기술을 수반하여 조직 구성원을 통제해야하고, 이는 조직 구성원들이 느끼는 스트레스에 영향을 미친다는 연구결과를 얻었다. 정보보안 관점에서 보안 인식교육은 보안 기술스트레스의 업무과중과 기술 불확실성에 유의한 관계를 가지는 것으로 나타났다. 즉 조직 구성원들을 대상으로 하는 정보보안 인식교육은 보안절차를 준수하도

록 통제하는 과정에서 업무 수행 절차가 추가됨으로써 자신의 업무가 과중되고 있다고 느끼는 것으로 분석되었다. 또한 정보보안 기술에 대한 도입으로 인해 기술의 발달이 진행되고 있음을 조직 구성원들이 느끼기에 나타난 결과라 할 수 있다. 또한 보안 기술스트레스는 보안정책 준수와 관계가 있는 것으로 나타났는데, 특히 주목할 점은 자신의 사생활이 기술로 인해 침해당하고 있다고 느끼거나 혹은 신기술로 인해 자신의 현재 직업상의 위치가 위협을 받는다고 느낄 경우 보안정책 준수를 유도하기 힘들다는 것이다. 정보보안 통제에 따른 스트레스가 정보보안에 영향을 미칠 수 있는 요인으로 규명됨에 따라 조직은 이러한 스트레스를 관리하기 위한 예방적 그리고 치유적 전략을 모두 활용할 것을 주장했다.

정보보안 통제와 성과는 상호간의 관련성이 있기 때문에 통제가 과도한 경우에는 불필요한 통제의 증가에 따른 비용 낭비, 업무 처리시간 증가 등의 비효율성이 발생하여 조직 구성원이 느끼는 보안 스트레스는 증가할 것이고, 과소 통제하게 되면 실질적 효과가 없는 통제로 인해 보안 스트레스는 감소할지라도 정보보안의 목적을 달성할 가능성이 희박하기 때문에 정보보안 통제의 정도는 정보보안 성과 및 보안 스트레스에 큰 영향을 미칠 수 있다.

제 3 절 정보보안 스트레스에 관한 선행연구 고찰

현대의 고도화된 산업사회에서 대부분의 인간은 직장에서 뿐만 아니라 사회 생활이나 가정생활에서도 스트레스를 받게 된다. 오늘날 직장인들은 새로운 지식과 정보, 과중한 업무량, 각종 공해와 위험한 작업환경, 자율권이 결여된 지나친 간섭, 의사결정에 참여하지 못하는 소외감, 경쟁

업체간의 반목, 상사·동료 및 고객과의 관계 등으로 많은 스트레스를 받게 된다. 또한, 급격한 환경 변화 하에서 기업은 생존, 유지, 발전하기 위하여 조직 구성원들에게 직무성과를 강조하고 지속적인 혁신과 도전을 요구하기 때문에 이러한 스트레스는 더욱 가중되고 있다.

스트레스의 개념을 인간에 최초로 적용한 Cannon(1929)은 유기체가 환경적인 스트레스 인자에 어떻게 반응하는가에 대해 깊은 관심을 갖고 있다. 그는 낮은 수준의 스트레스를 경험하였을 때는 견디어 낼 수 있지만, 그 정도가 심해지거나 지속될 때 생물학적 체계의 파괴를 야기하게 된다는 결론을 얻었다.

우리나라에서의 스트레스 연구는 1970년도 중반 병원 간호사들의 스트레스 자각증상에 대한 연구(이은옥 등, 1974)를 시점으로 산업의학, 가정 의학, 간호학 분야에서 주로 수행되어 왔다. 연구대상들은 주로 교대근무를 하는 간호사, 상점원, 기혼 직장 여성, 연구직 근로자, 산업장 근로자, 은행원, 약사 등 비교적 다양한 직종들을 대상으로 수행되었다. 또한 가정 의학 영역에서는 외래 환자들을 대상으로 스트레스의 기술적인 연구 등이 수행되었다. 우리나라 직장인들이나 지역사회 인구의 스트레스에 대한 유병률은 보고된 적이 없다. 현재의 우리나라에서의 스트레스 연구는 초기단계에 있으며, 우리나라 직장인들이나 지역 사회 주민들을 대상으로 한 스트레스에 의한 건강 영향 평가 등이 무엇보다도 시급한 연구 과제라 할 수 있다.

하지만, 증상으로서 스트레스는 모호하면서도 주관적이어서 개념 정의 및 측정상의 어려움이 존재해 왔던 것이 사실이다. 그동안 스트레스 개념의 복잡성, 다양성 등으로 인하여 스트레스에 대한 합의된 정의가 도출되지 못하였고, 이에 따라 표준화되고 객관적인 스트레스 측정도구가 개발되지 않아 스트레스가 질병 원인론이나 일상생활에서의 삶의 질

에 적지 않은 영향을 주고 있음에도 불구하고 이에 대한 체계적인 연구가 미흡했던 실정이다. 특히 국내의 경우, 국외에서 개발된 도구에 대한 신뢰도 검정이나 타당도 검정 등의 유용성 평가의 과정없이 그대로 번역하여 사용하여 왔으며, 연구내용에 있어서도 특정 집단 내에서의 스트레스 수준에 대한 기술적 분석만이 이루어졌다.

장세진(2000)은 그동안 외국에서 개발된 여러 가지의 스트레스 측정도구를 유용성 중심으로 평가하였고, 이를 토대로 우리 설정에 맞는 스트레스 측정도구를 개발하였다. 스트레스는 복합적 현상으로 스트레스로 인해 나타날 수 있는 결과는 다양하고, 동일한 수준의 스트레스 수준을 보였다하더라도 사람에 따라서 스트레스가 사람에게 미치는 영향이 다르게 나타날 수 있으므로 발생 가능한 스트레스의 차원을 측정도구에 포함하고, 신뢰도와 타당도 그리고 민감도에 있어 만족할 만한 측정도구로 평가되어진 Goldberg(1978)의 GHQ-60(General Health Questionnaire)을 토대로 스트레스 척도를 재구성하였다. 스트레스 요인을 사회적 역할 수행능력 및 자기신뢰, 우울증, 수면장해 및 불안, 그리고 일반 건강 및 생명력의 18항목으로 선정해서 사회·심리적 스트레스 측정도구(Psychosocail Well-being Index-Short Form)를 새롭게 개발하였다.

탁진국(2002)은 사무직, 생산직, 그리고 연구직이라는 서로 다른 직종에 따라 종업원들이 느끼는 직무스트레스원과 직무스트레스 정도에 어떤 차이가 있는지를 연구하였다. 세 집단 간의 비교 결과, 사무직은 다른 직종에 비해서 부서 갈등과 의사결정 참여를 상대적으로 더 큰 직무스트레스원으로 지각하였다. 자신이 생산할 제품에만 신경을 쓰는 생산직이나 자신의 전문적인 연구 분야에만 관심을 갖는 연구직에 비해서 사무직은 자신의 업무를 처리하는 과정에서 다른 부서와 접촉할 기회가 좀 더 많이 있기 때문에 이러한 과정에서 생기는 갈등이 큰 것으로 해석할 수 있

다. 생산직의 경우에는 상사관계, 직무불안정, 그리고 환경문제가 다른 직종보다 더 큰 직무스트레스원으로 작용하였다. 무엇보다 환경문제가 생산직에서 더 큰 직무스트레스원으로 나타난 것은 이들의 작업 환경이 사무직이나 연구직에 비해 열악하기 때문인 것으로 해석할 수 있다. 상사관계에 있어서도 일반적으로 사무직이나 연구직에 비해서 생산직 관리자는 감독을 좀 더 철저히 하고 업무에 대해 간섭하는 경우가 좀 더 많이 있기 때문에 생산직에서 더 큰 직무스트레스원으로 나타난 것으로 해석할 수 있다.

탁진국 등(2002)은 사무직 근로자를 대상으로 관리자와 일반사원에 대한 직무스트레스의 원인을 조직특성과 과정, 그리고 직무요구와 역할특성에 따라 연구했다. 이러한 직무스트레스원이 불안, 우울, 신체화와 같은 직무스트레스에 미치는 영향을 관리자와 일반사원 그룹으로 나누어 알아보았다. 그 결과 각 직무스트레스원들은 비교적 서로 독립적인 작용을 하는 것으로 판단되었으며, 두 집단을 비교해보았을 때 관리자 집단에서는 역할과다, 직무불안정, 그리고 일-가족 갈등이, 일반사원 집단에서는 역할갈등, 적성불일치, 의사결정참여, 그리고 승진문제가 유의한 직무스트레스원인 것으로 밝혀졌다. 또한 직무스트레스에 영향을 미치는 주요한 직무스트레스원으로는 관리자 집단의 경우, 적성 불일치, 직무 불안정, 그리고 일-가족 갈등인 것에 비해 일반사원 집단에 있어서는 역할과소, 동료만족, 그리고 환경문제가 직무스트레스에 중요한 영향을 미치는 것으로 나타났다. 이와 같은 결과는 직급에 따라 직무스트레스에 미치는 요인에 차이가 있음을 보여준다.

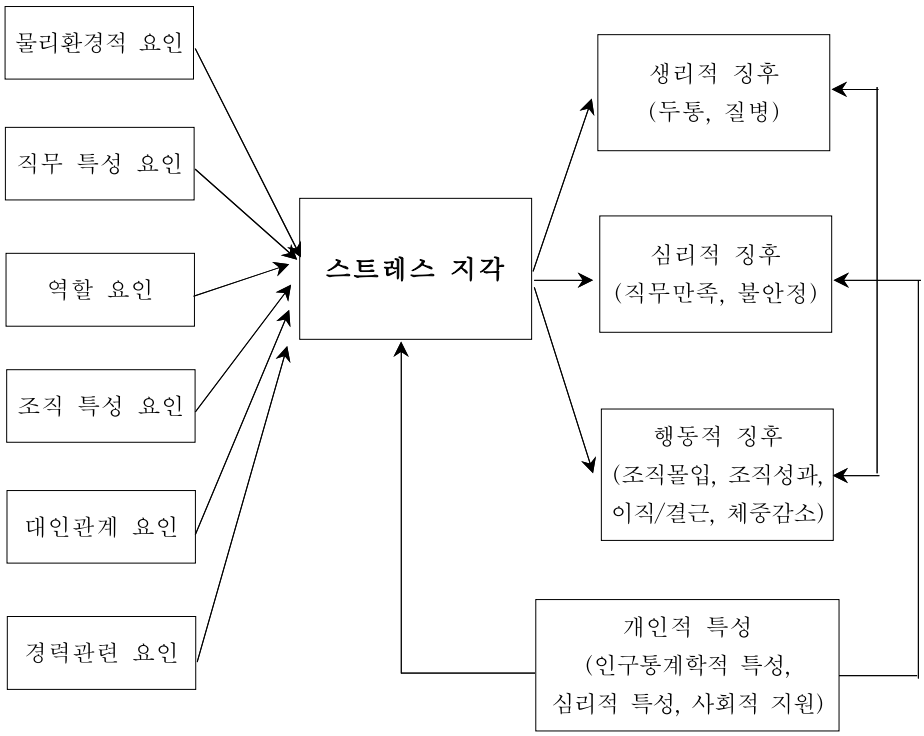
차경태 등(2008)은 사무직 근로자들의 스트레스와 피로수준을 연구하였는데, 사회 인구학적 특성에 따른 스트레스 수준을 비교한 결과 성, 연령, 결혼상태, 교육수준 모두에서 유의한 관련성을 보였다. 즉, 여자일수

록, 연령이 낮을수록, 미혼자일수록, 그리고 교육수준이 높을수록 스트레스 수준이 유의하게 높았다. 직업 특성별로는 대규모 사업장일수록, 정규직 일수록, 주 5일제 근무를 시행하지 않는 근로자일수록 스트레스 수준이 유의하게 높았다. 이러한 연구 결과는 일반적으로 직장인의 피로는 소규모 사업장의 근로자들이나 비정규직에서 높을 것이라는 예상되는 다소 상반된 결과를 보였는데, 이는 우리나라의 특수한 조직문화나 현재의 고용시장의 불안정성으로 설명되어 질 수 있을 것이다. 또한, 남자의 경우는 직무 스트레스의 하부 영역 중 직무 요구, 직무불안정성, 보상부적절 등이 영향력이 높은 주요 스트레스 요인이었던 반면, 여자는 보상부적절, 직장문화, 직무 요구도가 주요한 스트레스 요인으로 성별에 따라 직무 스트레스 하부 요인에 다소 차이가 있다는 것을 증명하였다.

박광희・유화숙(2003)은 스트레스에 관한 선행연구들를 종합적으로 분석하였다. 직무스트레스는 개인과 집단 및 조직 차원에서 조직구성원이 직무를 수행하는데 연관된 요인들에 정(+)적・부(-)적 영향을 주며, 이러한 직무스트레스는 직무와 관련된 환경 요인에 의해서 발생하며 개인적 특성에 따라 직무스트레스를 지각하는 정도가 다르다는 것을 알 수 있다. 조직 내의 직무스트레스 유발요인 및 조절 변인에 대한 논의는 연구자에 따라 그 분류가 다소 차이가 있으나, 직무스트레스의 요인 중 주로 밝혀진 7가지 요인은 물리적 환경요인, 직무특성요인, 역할관련요인, 조직특성요인, 대인관계요인, 경력개발요인, 개인적 요인 등으로 나타났다. 직무스트레스에 관한 선행연구에서 결과변인으로 측정되었던 변인들은 직무스트레스 지각, 직무성과, 직무만족, 직무몰입, 직무의 동기부여 잠재성, 조직 몰입, 이직성향, 결근의향, 불안정행동, 정신과적 증상, 심리적 긴장, 신체적 긴장, 정신적/신체적 고통 등이 있었다. 그 가운데서 직무스트레스 지각이 가장 많이 분석되었고 직무성과, 직무만족, 조직몰입,

이직성향 등이 대부분의 조사에서 분석되었다. 이외에도 조사대상자에 따라서 심리적 강인성, 여가활동, 생활의 불규칙성 등에 따른 직무스트레스 지각의 차이를 조사한 연구도 있었다. 선행연구들의 결과를 종합하여 <그림 2-2>와 같은 연구모형을 제시하였다.

<그림 2-2> 스트레스에 관한 연구 모형



지금까지의 스트레스에 관련된 선행연구를 살펴보면 주로 스트레스는 의학이나 생물학 그리고 사회심리학 분야에서 연구가 되었으나, 최근에는 스트레스의 문제가 종래의 한정적 학문분야를 벗어나 조직체의 중요한 문제로 부각되어 조직행동의 중요 영역으로 다루어지게 되었으며. 스트레스에 의해 발생하는 조직 내의 역기능적인 결과 때문에 직무 스트레스에 관한 연구와 그 관리 방안의 중요성이 부각되고 있다.

최근 기업들은 지속적으로 정보기술을 도입하여 ICT시스템이 기업 내에서 더욱 중요한 위치를 점하게 되는 계기가 되었다. ICT의 발전과 ICT 시스템의 보급은 많은 부작용을 발생시키고 있으며, 국내에서도 기업의 정보보안에 관련된 많은 유출 사건이 언론에 보도되어 경각심이 날로 높아지고 있는 실정이다. 이에 정보의 손실은 조직의 존망을 결정하는 가장 핵심적인 경쟁력이 되었고, 이에 따라 기업의 정보보안(Information Security)은 매우 중요한 요소가 되었다. 하지만, 정보보안 성과에만 치중하다보면 정보보안이 강화되고 정보보안 통제가 이루어질 수밖에 없다. 이에 따라 기업 구성원들이 업무에서 느끼는 불편함은 간과될 수 있다. 정보보안의 중요성은 당연히 인정하지만, 이로 인한 구성원들의 보안 스트레스는 점점 증가하고 있으며, 어떤 요인들로 인해 보안 스트레스가 증가하고 있는지 밝혀내고자 하는 것이 본 연구의 목적이다.

정보보안 스트레스와 관련된 선행연구를 살펴보면 이신권(2012)은 보안업무를 수행할 경우 느끼게 되는 신체적/심리적인 부정적인 반응 등을 보안피로도로 정의하였다. ICT보안 업무 종사자의 보안피로도와 다양한 결정요인(제도적, 기술적, 문화적, 개인적 요인)간의 인과관계를 분석한 결과, 전체적으로 보안피로도는 제도적 요인 종합지수, 기술적 요인 종합지수에 의해서 결정되는 것으로 나타났다. 즉 제도적 요인, 기술적 요인에 대한 부정적 인식이 높을수록 보안피로도에 대한 인식은 높은 것으로 나타났다. 그러나 보안피로도의 세부 항목별로 영향을 미치는 결정요인은 다소 차이가 있었다. 그리고 제도적, 기술적, 문화적, 개인적 요인의 하위 세부 항목별에 따라서 보안피로도 종합지수에 미치는 유의미한 요인에도 차이가 있는 것으로 나타났다.

박철주・임명성(2012)의 연구에서 보안 기술스트레스는 정보보안에 대한 개인의 부정적 인식인 인지된 효익(정보보안을 따르지 않았을 경우

개인이 느끼는 심리적 이익-업무시간 단축, 업무 생산성 증가 등)에 긍정적 영향을 미치는 것으로 나타났으며, 이는 조직에 대한 개인의 애착심에도 부정적 영향을 미치는 것으로 나타났다. 또한 보안인식을 위한 교육이 보안인식 고양과 기술적 대처방안에 치우치다보니 보안인식 교육은 보안 기술스트레스를 증가시키는 반면 개인의 정보보안에 대한 부정적 인식에는 아무런 영향을 미치지 못하는 것으로 나타났다. 반면 조직의 몰입에는 긍정적 영향을 미치는 것으로 나타났는데 이는 보안교육에도 조직에 대한 중요성을 강조하기 때문에 이로 인해 수반되는 영향이라 판단된다. 이러한 결과를 통해 조직은 어떻게 조직원들이 느끼는 기술적 스트레스를 감소시킬 것인지 고민해 보아야 한다. 즉 조직원들이 느끼는 기술적 스트레스를 지속적으로 평가하고 이를 감소시킬 수 있는 구체적인 방안을 수립하여 조직 전반에 걸쳐 실행해야 한다. 또한 정보보안 교육을 기술적 측면보다는 개인의 보안 인식의 고양에 초점을 맞춰 운영해야 한다. 보안 침해로 인해 기업이 받게 되는 잠재적 피해와 이러한 영향이 조직에 미칠 영향을 공유함으로써 조직원들 스스로 보안에 대한 중요성을 인식하게 해야 한다. 또한 보안 정책 수립 시 업무의 생산성과 보안 준수간의 상충관계를 고려한 절충안을 마련하여 보안 준수와 생산성 하락간의 부정적 인식을 전환시킬 필요가 있다. 뿐만 아니라 보안 정책상 업무의 단절을 야기할 수 있는 상황을 고려하여 이를 개선할 수 있는 방안을 마련하여 조직원들의 업무단절이 최소화될 수 있도록 조직차원의 노력이 필요하다.

신호영(2013)은 스마트폰 사용자에 대한 정보보안 행위의도에 대한 요인을 분석하였다. 스마트폰 악성코드인 스파이웨어에 대한 문제해결 방안으로 설치하는 백신프로그램에 대해서 스마트폰 이용자들의 관심도가 높을수록 이용자들의 사용의도는 높아지고 이로 인해 이용자들은 정보보

안에 대한 스트레스가 낮아지는 것으로 분석되었다. 자신이 어떤 일이나 상황에 처했을 때 평소에 관심을 가지고 있던 분야에 대해서 내가 잘해 낼 수 있을 것이라는 자신의 능력에 대한 신뢰와 믿음을 통해 정보보안 행위에 대한 의도가 증가하고, 스트레스는 감소시킬 수 있는 것이다.

이장호(2013)는 정보보안 스트레스 요인으로 조직특성, 기술능력, 보상제도로 구분하였다. 엄격한 보안문화 및 보안업무 담당자의 고압적인 업무 태도는 보안 스트레스에 영향을 미치는 것으로 분석되었다. 계속에서 발전하고 있는 ICT기술과 비례하여 증가하고 있는 ICT 보안능력 및 기술이 보안 스트레스에 영향을 미치는 것으로 나타났다. 이렇게 정보보안 스트레스를 증가시키는 요인이 있는 반면, 보상제도는 보안 스트레스를 경감시킬 수 있는 요인으로 분석되었다.

다양한 분야에서 스트레스에 관한 연구는 진행되어 왔으나, 정보보안 분야에서의 스트레스 연구는 미흡하다. ICT의 발전으로 의존도가 높아지고, 이를 위해 정보통신시스템에 대한 관리·통제에 관한 정보보안이 중요한 이슈로 대두되고 있는 상황에서 과도하고 불필요한 정보보안 통제 및 감시 활동은 업무의 비효율성을 초래할 뿐만 아니라 조직 구성원에게 스트레스를 유발시킬 수 있다. 정보보안의 중요성은 당연히 인식하지만, 이로 인한 정보보안 스트레스는 간과되어지고 있다. 본 연구에서는 정보보안 분야별(기술적, 물리적 및 관리적)로 조직 구성원이 느끼는 스트레스를 측정하기 위해 업무를 수행함에 있어 보안 요구사항이 조직 구성원의 능력이나, 지원, 바램과 일치하지 않을 때 생기는 유해한 신체적/정서적 부정적 반응을 보안스트레스로 정의하고, 정보보안 분야별 보안 스트레스 결정요인에 대해 연구하고자 한다.

제 3 장 연구모형 및 가설

제 1 절 연구 모형의 설계

1. 연구문제

본 연구는 선행연구 검토에서 언급한 조직구성원의 특성 중 개인적 요인(보안관심도), 회사환경요인(전략신뢰도, 보안 교육수준), 직무특성요인(근무분야, 직위, 근무지)이 정보보안 분야별 보안 스트레스(기술적, 물리적, 관리적)에 어떠한 영향을 미치는지 분석하고자 한다.

연구문제 1: 보안관심도는 정보보안 스트레스에 어떠한 영향을 미치는가?
연구문제 2: 전략신뢰도는 정보보안 스트레스에 어떠한 영향을 미치는가?
연구문제 3: 보안 교육수준은 정보보안 스트레스에 어떠한 영향을 미치는가?
연구문제 4: 보안업무 담당 여부는 정보보안 스트레스에 어떠한 영향을 미치는가?
연구문제 5: 회사 내 직위는 정보보안 스트레스에 어떠한 영향을 미치는가?
연구문제 6: 근무지는 정보보안 스트레스에 어떠한 영향을 미치는가?

2. 연구모형

본 연구에서는 보안 업무 수행 시 느끼게 되는 신체적, 심리적 부정적인 반응을 보안 스트레스로 정의하고, 보안 스트레스의 주요 요인들은 정보보안 목적을 달성하기 위한 각 분야별로 영향을 미칠 것으로 예상하고 각각의 스트레스 형태로 구분하였다. 앞서 제시한 선행연구 검토를

통해 정보보안 요소들은 기술적 보안, 물리적 보안 및 관리적 보안으로 구분하였다. 기술적 보안, 물리적 보안, 관리적 보안의 성과를 달성하기 위해 통제활동이 이루어지고 조직구성원들에게는 많은 부담으로 작용하여 각각의 정보보안 스트레스 형태로 나타날 것으로 예상된다.

정보보안 분야별 스트레스에 영향을 미치는 요인으로 본 연구에서는 선행연구들을 고찰하여 조직구성원의 특성을 크게 세 가지로 구분하였다. 첫째로 조직구성원의 개인적 특성이 정보보안 스트레스에 미치는 영향을 살펴보고자 한다. 개인적 요인인 보안관심도는 조직구성원들이 정보보안에 대해 관심을 가지고 있는 태도의 한 형태로서 정보보안에 관심이 있어 하는 심리적 상태를 말한다. 개인의 보안 지식정도에 따라 차이를 보이는 보안관심도는 정보보안 스트레스의 하나의 요인이 될 수 있다.

두 번째로 조직구성원의 회사환경적 특성이 정보보안 스트레스에 미치는 영향을 살펴보고자 한다. 회사환경적 특성은 회사의 보안정책에 대한 전략신뢰도와 회사에서 시행하는 정보보안 교육에 대한 수준으로 구분된다. 회사 보안 전략신뢰도는 조직구성원들이 자신이 속한 조직 및 조직목표・전략에 대한 신뢰감을 느끼고 조직구성원으로서 따르려고 하는 태도 뜻하며, 회사 보안 교육수준은 조직구성원들이 자신이 속한 조직의 교육정책 및 교육역량에 대해 느끼는 상태를 말한다.

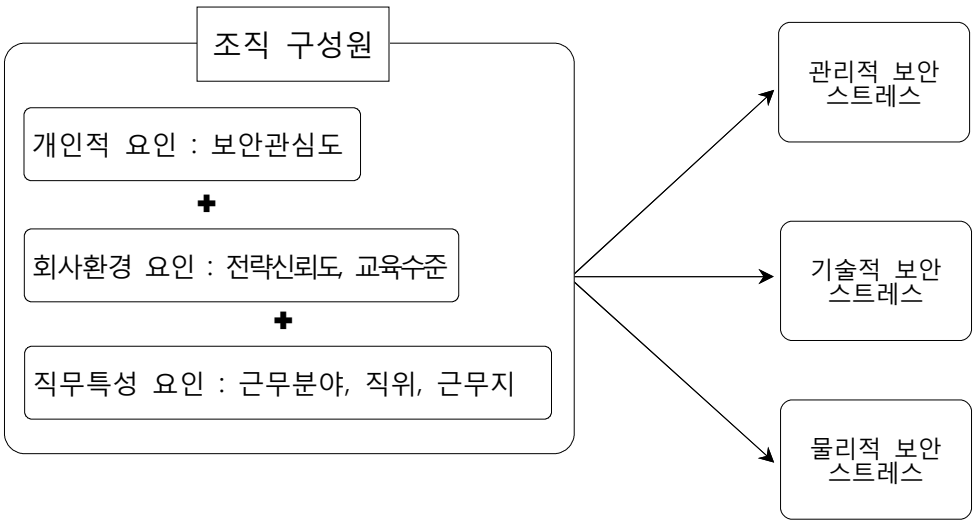
마지막으로 직무특성 요인을 근무분야, 회사 내 직위, 근무지로 구분하였다. 근무환경 측면에서 근무분야는 보안업무 담당 여부를 의미하며 ICT보안 업무 종사자와 일반 사무직 종사자로 구분하여 연구하고자 한다. 본 연구의 대상인 K공사에서 ICT보안 업무 종사자의 임무는 크게 다섯 가지로 나누어진다. 첫째는 정보보안 정책 및 활동 세부계획 수립이다. 둘째는 정보보안 업무 감사・지도・감독 및 교육이다. 셋째는 정보

보안 사고조사, 복구 및 처리이다. 넷째는 정보보안관련 지침 등 제도 개선이다. 다섯째는 ICT시스템 보안 대책 검토 및 지도 감독이다. 이러한 업무를 다루지 않는 조직 구성원은 일반 사무직 종사자로 구분한다. 즉, 보안시스템을 도입하고 정책을 수립하는 ICT보안 업무 종사자와 그 시스템을 사용하고 정책을 따르는 일반 사무직 종사자로 구분하여 각각이 느끼는 보안 스트레스와 그 차이를 분석하고자 한다.

또한, 회사 내 직위는 간부여부를 의미한다. 즉 일반 직원과 간부 간에 느끼는 보안 스트레스에 차이가 있는지를 분석하고자 한다. 노동조합에 속해 있는 일반 직원과 일반직원들의 관리자 역할을 맡고 있을 뿐만 아니라, 노동조합에 속하지 않고 회사 간부로 속해 있는 3직급 이상의 직원들이 느끼는 보안 스트레스를 비교하여 그 차이를 분석하고자 한다. 근무지는 본사 근무 여부를 의미하며, 본사와 사업소로 구분하여 각각의 소속지에서 느끼는 보안 스트레스에 차이가 있는지를 분석하고자 한다.

정보보안 이론 및 선행연구들을 고찰하여 보안스트레스에 미치는 영향을 실증적으로 규명하고자 <그림 3-1>과 같은 연구모형을 설정하였다.

<그림 3-1> 보안 스트레스에 미치는 영향을 측정하기 위한 연구모형



제 2 절 연구가설의 설정

본 연구에서는 앞서 제시한 연구모형과 이론적 고찰을 배경으로 조직 구성원들이 보안업무에 대해서 느끼는 정보보안 스트레스(기술적, 물리적, 관리적 보안 스트레스)를 종속 변수로 설정하고, 그 원인을 알아보기 위한 독립변수를 개인적 요인(보안관심도), 회사환경 요인(전략신뢰도/보안교육수준), 직무특성 요인(근무분야/직위/근무지)으로 나누고, 세부적으로는 총 6가지 변수를 설정하였다. 독립변수와 종속변수의 인과관계를 통계적으로 검증하기 위해 다음과 같이 연구 가설을 설정하였다.

가설 1. 조직 구성원의 특성은 기술적 보안 스트레스에 영향을 미칠 것이다.
1-1. 보안관심도가 높을수록 기술적 스트레스에 부(-) 영향을 미칠 것이다.
1-2. 전략신뢰도가 높을수록 기술적 스트레스에 부(-) 영향을 미칠 것이다.
1-3. 보안교육수준이 높을수록 기술적 스트레스에 부(-) 영향을 미칠 것이다.
1-4. 보안업무 담당 여부는 기술적 스트레스에 부(-) 영향을 미칠 것이다.
1-5. 회사 내 간부 여부는 기술적 스트레스에 부(-) 영향을 미칠 것이다.
1-6. 본사 근무 여부는 기술적 스트레스에 부(-) 영향을 미칠 것이다.

연구가설1은 조직구성원의 개인적, 회사환경, 직무특성 요인과 기술적 정보보안 스트레스 사이의 관계를 설명하는 것이다. 첫 번째 개인적 요인인 보안관심도는 개인의 보안 지식 정도에 따라 느끼는 기술적 보안 스트레스에 차이가 있는지를 검증하는 것이다. 개인마다 경험과 처한 상황이 달라 그에 따른 정보보안 지식도 다를 것이다. 예전에 정보보안 사고 경험이 있다면 그 경험 이후에 보안에 관한 관심도 증가로 보안 지식이 증가하고 이를 통해 ICT보안 기술을 습득하여 기술적 보안 스트레스가 감소할 수 있다. 반대로 정보보안 사고 경험으로 보안 관심도는 증가

할 수 있으나, 이로 인해 기술적 보안 스트레스는 증가할 수 있다. 사용자 심리적 특성과 스트레스와의 관계(박광희 등, 2003), 정보보안 사용통제와 사용자 관심도와의 관계(김종기 등, 2006) 등이 보고되고 있어, 보안 관심도는 기술적 보안 스트레스와 높은 관련성이 있을 것으로 판단된다.

다음으로 회사 보안 전략신뢰도 및 보안 교육수준과 기술적 보안 스트레스간의 관계를 검증하고자 한다. 선행연구들을 살펴보면 보안 전략신뢰도와 교육수준이 높을수록 기술적 보안 스트레스에 부(-)의 영향을 미치는 것으로 보이고 있다.(박철주・임명성, 2012)

직무특성 요인으로 보안업무 담당 여부는 보안업무 종사자와 비관련 종사자 집단 간의 보안 스트레스에 차이가 있는지를 검증하는 것이다. ICT보안업무 종사자는 자신의 고유의 업무이므로 보안 스트레스를 지각하는 수준이 일반 사무직 종사자보다 낮을 수 있다. 이러할 경우 ICT보안업무 종사자는 보안 성과달성을 위해 무분별한 통제 정책을 시행할 수 있고, 이로 인해 발생하는 일반 사무직 종사자의 보안 스트레스를 간과할 수 있다. 박상서 등(2008)은 적정 수준의 보안에 관해서는 일반 조직구성원과 보안담당자 사이에 간격이 있음을 발견하였고, 그를 통해 조직에서는 사용하는 전략간에 균형을 맞추어야 하며, 조직의 임원과 직원/보안담당자간에 보안 수준에 관하여 동의가 필요하다고 하였다.

직무특성 요인의 두 번째로 회사 내 직위, 즉 일반 직원과 간부간에 느끼는 보안 스트레스에 차이가 있는지를 검증하는 것이다. 노동조합에 속해있는 일반 직원과 회사 간부로 속해있는 3직급 이상의 직원들이 느끼는 보안 스트레스를 비교하여 그 차이를 분석하고자 한다. 회사 간부들은 회사에 대한 책임감 및 충성도가 일반 직원들에 비해 높으므로 과도한 정보보안 통제 정책이 있더라도 이에 순응하여 그들이 체감하는 스

트레스는 일반 직원에 비해 낮을 수 있을 것이다.

세 번째로 근무지를 본사와 지역본부 즉, 사업소로 나누고 두 집단간에 느끼는 정보보안 스트레스에 차이가 있는지를 검증하는 것이다. 본사의 경우 대부분의 주요 회사 정보를 보유하고 있어 사업소보다 정보보안 강도가 높을 것이고, 또한 본사에 근무하는 대부분의 직원이 정보보안의 중요성을 인식하고 있을 것으로 예상되어 사업소 직원과는 그 스트레스에서 차이가 있을 것으로 예상된다.

가설 2. 조직 구성원의 특성은 관리적 보안 스트레스에 영향을 미칠 것이다.
2-1. 보안관심도가 높을수록 관리적 스트레스에 부(-) 영향을 미칠 것이다.
2-2. 전략신뢰도가 높을수록 관리적 스트레스에 부(-) 영향을 미칠 것이다.
2-3. 보안교육수준이 높을수록 관리적 스트레스에 부(-) 영향을 미칠 것이다.
2-4. 보안업무 담당 여부는 관리적 스트레스에 부(-) 영향을 미칠 것이다.
2-5. 회사 내 간부 여부는 관리적 스트레스에 부(-) 영향을 미칠 것이다.
2-6. 본사 근무 여부는 관리적 스트레스에 부(-) 영향을 미칠 것이다.

연구가설2는 조직구성원의 개인적, 회사환경, 직무특성 요인과 관리적 정보보안 스트레스 사이의 관계를 설명하는 것이다. 관리적 측면의 정보보안에 대한 선행 연구 결과들(정구헌 등, 2011; 이장호 2013))을 살펴보면 회사 보안 전략신뢰도는 관리적 보안 스트레스에 부(-)의 영향을 미치는 것으로 나타났다. 조직 구성원이 회사의 정책에 대해 기본적으로 불신을 가지고 있다면, 이러한 선입견으로 인해 회사가 아무리 좋은 정보보안 대책을 제시하여도 조직 구성원들은 이를 신뢰하지 않을 것이고, 이로 인해 관리적 보안 스트레스가 증가하게 될 것이다.

특히 보안관심도는 보안 전략신뢰도와 결합하여 기업의 정보보안 관리에 시너지를 이끌어 내는 것으로 나타났다.(김종기 등, 2006) 보안 전

략은 현재 보유한 ICT능력을 활용할 뿐만 아니라 새로운 ICT보안 기술에 대한 지속적인 관심, 탐색과 시도를 통해 정보보안 관리 능력을 향상시키는데 긍정적 영향을 미치고 있다.

회사 보안 교육을 통하여 조직 구성원 각자가 경험한 보안 교육에 의해 보안 지식이 늘어나 긍정적인 효과를 일으킬 수도 있지만, 반면에 그 교육으로 인한 맹목적 교육 수강으로 오히려 스트레스가 늘어날 수도 있다. 선행 연구 결과들(박준형, 2008; 이신권 2012)을 살펴보면, 보안 교육 수준이 높을수록 관리적 보안 스트레스에 부(-)의 영향을 미치는 것으로 분석되었지만, 본 연구에서는 다른 요인들을 추가했을 때도 동일한 결과가 나오는지를 재확인하고자 한다.

가설 3. 조직 구성원의 특성은 물리적 보안 스트레스에 영향을 미칠 것이다.
3-1. 보안관심도가 높을수록 물리적 스트레스에 부(-) 영향을 미칠 것이다.
3-2. 전략신뢰도가 높을수록 물리적 스트레스에 부(-) 영향을 미칠 것이다.
3-3. 보안교육수준이 높을수록 물리적 스트레스에 부(-) 영향을 미칠 것이다.
3-4. 보안업무 담당 여부는 물리적 스트레스에 부(-) 영향을 미칠 것이다.
3-5. 회사 내 간부 여부는 물리적 스트레스에 부(-) 영향을 미칠 것이다.
3-6. 본사 근무 여부는 물리적 스트레스에 부(-) 영향을 미칠 것이다.

연구가설3은 조직구성원의 개인적, 회사환경, 직무특성 요인과 물리적 정보보안 스트레스 사이의 관계를 설명하는 것이다. 정보시스템이 위치한 정보처리시설을 보호하기 위한 정보보안 통제에 의해 유발되는 스트레스가 물리적 보안 스트레스이다. 물리적 측면의 정보보안에 대한 선행 연구 결과들(이신권, 2012; 신호영 2013)을 살펴보면 보안관심도 및 회사 보안 전략신뢰도는 물리적 보안 스트레스에 부(-)의 영향을 미치는 것으로 나타났다. 보안에 대한 충분한 지식과 이해가 부족하다면 조직차원의

물리적 보안 조치에는 한계가 있다. 조직구성원을 중심으로 충분한 보안 교육과 주의에 대한 환기가 요구된다. 즉, 개인적 차원에서 정보보안관련 지식과 경험은 정보보안 활동과 상호작용하여 구성원들의 행태에 대한 변화와 자극을 촉진하게 된다. 보안에 대한 관심도가 높을수록 정보보안 지식의 수준이 높아지고 그에 따라 정보보안 행동이 촉진되어 정보보안 행동의 수준을 높이고, 이에 따라 보안 스트레스는 감소하게 될 것으로 예상한다.

하지만, 불편한 업무프로세스가 진행되어 업무의 효율성을 낮추는 물리적 보안 스트레스의 특성상 개인적, 회사환경 및 직무특성 요인에 의해 영향을 받더라도 다른 두 가지 보안 스트레스(기술적, 관리적)보다 가장 작은 영향을 받을 것으로 예상된다.

제 3 절 연구의 대상 및 분석방법

1. 연구의 대상 및 변수의 정의

가. 연구의 대상

본 연구에서 주된 연구 대상은 공기업인 K공사 구성원들의 보안 스트레스 수준과 보안 스트레스에 영향을 미치는 요인들을 분석하기 위해 설문조사를 시행한다.

본 연구의 실증 분석에서는 K공사 본사 및 전국 각지의 사업소를 대상으로 실증적 분석을 실시했으며, 대상 사업소의 범위는 1차사업소 및 3급 이상 2차 사업소로 한정했다. 왜냐하면 지역 서비스센터 등 3급 이

하 사업소는 사업소장을 제외한 조직구조가 수평조직에 가깝고 조직구성원 측면에서도 해당지역 출신 인사가 많이 배치되어 있는 등 일반적인 공사조직의 특성과 많이 다르기 때문이다. 따라서 사업본부 및 3급 이상의 사업소로 분석대상을 제한함으로써 연구의 효율성을 기하였다. 연구대상 조직 및 인원은 본사 및 3개 사업본부 25개 팀 300명을 표본대상으로 하여 설문조사를 시행하였다. 설문지 조사는 입사 6개월 이상인 직원을 대상으로 설문지를 배포하여 통계분석을 실시하였다.

조사대상인 3개의 사업본부는 수도권 지역과 지방 각 2개소로 하였다. 이는 지역별 특성을 다양하게 포함하여 연구결과가 다양한 사업본부로 일반화할 수 있도록 하고, 또한 3개 사업본부를 비교하여 상대적으로 체감하는 보안스트레스 등 보다 깊이 있는 연구를 위함이다.

나. 종속변수

종속변수인 각 분야별 정보보안 스트레스는 정보보안에 대한 선행연구들(이선중・이미정, 2008; 남길현・원동호, 2010)을 토대로 정의하였다. 첫째, 기술적 보안 스트레스는 보안기술, 소프트웨어, 응용 프로그램 등에 의한 통제로 인해 조직구성원들이 체감하는 신체적, 정서적 부정적 반응의 정도를 의미한다. 둘째, 관리적 보안 스트레스는 보안계획, 보안지도, 보안감사 등에 의한 통제로 인해 조직구성원들이 체감하는 신체적, 정서적 부정적 반응의 정도를 의미한다. 셋째, 물리적 보안 스트레스는 PC, 건물 등에 물리적 접근, 접속 차단에 의한 통제로 인해 조직구성원들이 체감하는 신체적, 정서적 부정적 반응의 정도를 의미한다.

본 연구에서 기술적, 물리적 및 관리적 보안 스트레스는 공기업인 K

공사의 정보보안 실태 평가 항목들 중 ICT보안 업무 종사자와 일반 사무직 종사자 모두에게 해당하는 부분을 사용하였다. 종속변수관련 항목은 아래 <표 3-1>과 같다. 아래의 항목을 참고로 하여 각각의 분야별로 느끼는 보안 스트레스를 측정할 수 있는 설문을 작성하였다.

<표 3-1> K공사 정보보안 실태 평가 항목

구분	세부 점검사항	비고
정보보안 기본활동	정보보안 감사・점검・지도방문을 실시하는가?	관리적 보안
	정보보안 교육을 실시하고 있는가?	관리적 보안
	사이버・보안 진단의 날을 내실있게 수행하는가?	관리적 보안
	업무자료를 상용 전자우편으로 전송하고 있지 않는가?	물리적 보안
	용역업체 직원의 내부 정보통신시스템 접근을 통제하고 있는가?	물리적 보안
PC 및 서버 보안관리	PC・서버에 설치된 운영체제 및 응용프로그램을 최신 보안 업데이트 하였는가?	기술적 보안
	백신프로그램이 자동 업데이트되고 실시간 감시기능이 설정되어 있는가?	기술적 보안
	내PC지키미를 실행하여 관리하고 있는가?	기술적 보안
	인가받지 않은 휴대용 저장매체(USB메모리, 이동형 하드디스크 등)를 반입・휴대하고 있는가?	물리적 보안
	비밀번호 설정시 특수문자 포함, 9자리 이상으로 설정하고 주기적으로 변경 사용하는가?	관리적 보안
정보통신 시설보안	외부인의 정보통신실 출입이 통제되고 관련 기록이 관리되는가?	물리적 보안
	외부인이 사옥내 출입할 경우 출입통제를 실시하고 있는가?	물리적 보안
	사무실 책상서랍 등에 비밀문건이나 비인가 정보통신 기기가 방치되어 있는지 주기적으로 확인하는가?	관리적 보안

기술적 정보보안 스트레스는 “내PC지키미[4]의 의무실행으로 인해 부담감을 느낀다.” 등의 5개 항목을 질문하여 “전혀그렇지않다.(1점)”에서 “매우그렇다.(5점)의 5점 리커트 척도로 측정하였다. 5개의 기술적 정보보안 스트레스의 평균을 합산한 점수를 종속변수인 기술적 스트레스 변수의 값으로 삼았다.

물리적 정보보안 스트레스는 “보안SUB[5] 사용으로 스트레스를 받는다.” 등의 5개 항목을 질문하여 “전혀그렇지않다.(1점)”에서 “매우그렇다.(5점)의 5점 리커트 척도로 측정하였다. 5개의 물리적 정보보안 스트레스의 평균을 합산한 점수를 종속변수인 물리적 스트레스 변수의 값으로 삼았다.

관리적 정보보안 스트레스는 “매월 시행하는 사이버 보안 진단의 날로 인해 스트레스를 받는다.” 등의 5개 항목을 질문하여 “전혀그렇지않다.(1점)”에서 “매우그렇다.(5점)의 5점 리커트 척도로 측정하였다. 5개의 관리적 정보보안 스트레스의 평균을 합산한 점수를 종속변수인 관리적 스트레스 변수의 값으로 삼았다.

다. 독립변수

정보보안 스트레스의 영향요인은 측정방법에 따라서 많은 요인들이

---

4) 내PC지키미 : 정부 공공기관에 근무하는 공무원들이 보안 점검을 손쉽게 할 수 있도록 국가정보원이 제공하는 보안 점검 소프트웨어(SW)이다. PC점검, 패스워드점검도구, PC 정리, 보고서 보기 등으로 크게 구성돼 있고 부수적으로 자주하는 질문에 대한 답변, 프로그램 정보 등도 제공한다.

5) 보안USB(Security Universal Serial Bus) : 정보유출방지 등의 보안 기능을 갖춘 USB 메모리이다. 모든 보안 USB는 필수적으로 사용자 식별·인증, 지정데이터 암·복호화, 저장된 자료의 임의복제 방지, 분실 시 데이터 보호를 위한 삭제 4가지 기능을 갖추어야 한다.

작용하겠지만, 그것들을 모두 연구모형에 포함시키기에는 무리가 있으므로 선행연구에서 다루어졌던 변수들과 조직구성원들의 특성을 고려하여 독립변수를 크게 개인적 요인, 회사환경 요인, 직무특성 요인 이렇게 3가지로 구분하고, 세부적으로는 총 6가지 변수를 설정하였다. 개인적 요인은 보안관심도로 설정하였고, 회사환경 요인으로는 회사 보안 전략신뢰도와 회사 정보보안 교육수준으로 설정하였다. 마지막으로 직무특성 요인은 보안업무 담당 여부(근무분야), 회사 내 간부 여부(직위), 본사 근무 여부(근무지)로 정하였다. 각 독립변수 중 개인적 요인과 회사환경 요인은 설문을 통해 분석하였으며, 설문지 구성 및 출처는 <표 3-2>와 같다.

<표 3-2> 독립변수 설문지의 구성 및 출처

구분	변수이름	측정항목	측정항목 출처
개인적 요인	보안관심도	5	김종기 등(2006) 신호영(2013)
회사환경 요인	회사 보안 전략신뢰도	5	백민정(2010) 박철주 등(2012) 이장호(2013)
	회사 보안 교육수준	7	박준형(2008) 이신권(2012)

개인적 요인 측면에서의 보안관심도는 조직구성원들이 정보보안에 대해 관심을 가지고 있는 태도의 한 형태로서 정보보안에 관심이 있어 하는 심리적 상태를 말한다. 이것을 측정하기 위해 선행연구들(김종기 등, 2006; 신호영 2013)이 제시한 척도를 참고하여 적용하였다. 세부내용으로 시사뉴스, 관련지식, 정보보안 소통의지 등 다섯 가지 측정 항목을 적용

하였다.

회사 보안 전략신뢰도는 조직구성원들이 자신이 속한 조직 및 조직목표・전략에 대한 신뢰감을 느끼고 조직구성원으로서 따르려고 하는 태도를 말한다. 이것을 측정하기 위해 선행연구들(백민정 2010; 박철주 등, 2012; 이장호, 2013)이 제시한 척도를 참고하여 적용하였다. 세부내용으로 정보보안 담당자, 정보보안 방지 대책, 타 공공기관과 비교 등 다섯 가지 측정 항목을 적용하였다.

회사 보안 교육수준은 조직구성원들이 자신이 속한 조직의 교육정책 및 교육역량에 대해 느끼는 상태를 말한다. 이것을 측정하기 위해 선행연구들(박준형, 2008; 이신권, 2012)이 제시한 척도를 참고하여 적용하였다. 신입직원, 방법론, 교육량 등 7가지 측정 항목을 적용하였다.

직무특성 요인 독립변수인 근무분야, 즉 보안업무 담당여부는 ICT보안 업무 종사자와 일반 사무직 종사자 2개의 집단으로 구분하였다. 회사 내 직위는 노동조합에 속해 있는 4직급 이하 직원을 일반 직원으로, 회사 간부로 속해있는 3직급 이상의 직원들로 구분하여 정하였다. 근무지에 관한 구분은 본사 및 3개 사업본부을 표본대상으로 하였다. 하지만, 본 연구에서는 주요 회사 정보를 보유하고 관리하는 본사에서 근무 여부가 정보보안 스트레스에 미치는 영향을 분석하고자 하는 것이기 때문에 본사와 사업소로만 구분하였다.

라. 통제변수

통제변수는 인구사회학적 변수로서 성별, 연령, 교육정도(최종학력)로 정하였다. 차경태 등(2008)의 연구를 통해 밝혀졌듯이 인구사회학적 특

성도 스트레스에 영향을 미치지만, 본 연구에서는 통제변수로 설정하였다.

K공사의 정보보안 평가 항목들로부터 추출된 종속변수인 기술적, 관리적, 물리적 정보보안 스트레스와 설문을 통해 조사한 독립변수인 개인적 요인, 회사환경 요인, 직무특성 요인 등의 조직구성원 특성과 성별, 연령, 교육정도로 구분된 사회인구학적 배경인 통제변수를 최종 정리하면 아래 <표 3-3>과 같다.

<표 3-3> 연구변수의 정의

변수기능	변수군	변수이름
통제변수	사회인구학적 배경	성별
		연령
		교육정도
독립변수	개인적 요인	보안 관심도
	회사환경 요인	회사 보안 전략 신뢰도
		회사 보안 교육수준
	직무특성 요인	근무분야
		직위
		근무지
종속변수	정보보안 스트레스	기술적 보안 스트레스
		물리적 보안 스트레스
		관리적 보안 스트레스

2. 연구 분석방법

본 연구의 가설을 실증적으로 분석하기 위하여 회수된 설문지 자료에 대한 부호화(Coding) 과정을 수행하고 SPSS 통계 패키지를 이용하여 분석을 시행하였다.

첫째, 인구통계학적 변수에 대한 현황과 부가 질문에 대한 빈도분석(Frequency Analysis)을 통해 파악하고, 둘째, 실증분석에서 조사도구의 신뢰성(Reliability)과 타당성(Validity)이 중요하기 때문에 앞에서 설정한 독립변수들과 종속변수들이 통계적인 타당성과 신뢰성이 있는지 확인하기 위해 신뢰도 분석(Cronbach-α 테스트)과 요인분석(Factor Analysis)을 실시하였다. 또한 변수간의 상관관계(Correlation)를 분석하기를 규명하기 위해 상관관계 분석을 실시하였다. 마지막으로 연구가설을 검증하고자 다중회귀분석(Multiple Regression Analysis)을 실시하였다. 각 항목별 연구 분석 방법은 아래 <표 3-4>와 같다.

<표 3-4> 연구 분석방법

내용	분석방법
Ⅰ. 인구통계학적 변수 분석	빈도분석
Ⅱ. 설문지 문항분석(신뢰도 검증)	신뢰도 분석
Ⅲ. 설문지 문항분석(타당도 검증)	요인분석
Ⅳ. 설문지 문항분석(상관관계 검증)	상관관계 분석
Ⅴ. 가설1	다중회귀분석
Ⅵ. 가설2	다중회귀분석
Ⅶ. 가설3	다중회귀분석

제 4 장 분석결과 및 논의

제 1 절 표본의 일반적 특성

본 연구에서는 K공사의 본사와 3개 지역본부에 근무하는 직원들을 표본 집단으로 선정하여 조사항목에 대해 응답자의 주관적 인식을 설문함으로써 자료를 수집하였다. 연구조사를 위해 전체 300부의 설문지의 설문지를 배포하여 265부를 회수하였으며, 이 중 응답이 비논리적이거나 지나치게 불성실한 25부를 제외한 240부가 분석에 사용되었다.

연구를 위해 수집된 응답자의 인구통계학적 특성 중 성별과 결혼여부을 살펴보면 다음의 <표 4-1>과 같다. 응답자 중 남성이 181명(75.5%), 여성은 59명(24.5%)으로 상대적으로 남성 응답자의 비율이 높은 편이었다. 하지만, K공사의 임직원 19,506명('13년 4월 기준) 중 남성 직원 비율이 84.5%인 것에 비하면 비교적 고르게 샘플링된 것이라 할 수 있다.

<표 4-1> 설문대상의 성별 및 결혼여부

성 별	빈 도	비율(%)	결 혼	빈 도	비율(%)
남	181	75.5	기 혼	177	73.6
여	59	24.5	미 혼	63	26.4
합계	240	100	합계	240	100

응답자의 연령대에 있어 40대 이상 82명(34.5%), 30대 116명(48.2%)으로 전체의 82.7%를 차지하였으며, 그 외에 20대 42명(17.3%)으로 응답

비율을 나타내었다. 이는 K공사의 임직원 통계와는 다소 상이한 것으로 실제로 40대 이상은 62.5%, 30대는 31.3%, 20대리하는 6.2%로 구성되어 있다. 본 연구에서는 K공사의 연령대 평균 분포보다 다소 젊은 직원들이 설문에 응했다고 볼 수 있다. 설문대상의 연령대는 다음 <표 4-2>와 같다.

<표 4-2> 설문대상의 연령

구 분	빈도	퍼센트	유효 퍼센트	누적 퍼센트
20대	42	17.3	17.3	17.3
30대	116	48.2	48.2	65.5
40대 이상	82	34.5	34.5	100.0
합 계	240	100.0	100.0	

그 외의 인구통계학적 특성으로 설문대상의 최종학력을 살펴보면 대졸자가 181명(75.5%), 석사학위자가 59명(24.5%)을 차지하였으며, 근무지를 살펴보면 본사 근무자가 135명(56.4%), 사업소 근무자가 105명(43.6%)을 차지하였다. 설문대상의 최종학력과 근무지는 다음 <표 4-3>과 같다.

<표 4-3> 설문대상의 최종학력 및 근무지

최종학력	빈 도	비율(%)	근무지	빈 도	비율(%)
대졸	181	75.5	본사	135	56.4
석사	59	24.5	사업소	105	43.6
합계	240	100	합계	240	100

이는 K공사의 임직원 통계와는 다소 상이한 것으로 실제로 대졸자는 58.1%, 석사학위자는 9%로 구성되어 있고, 본사 근무자는 9.8%, 사업소 근무자는 90.2%로 구성되어 있다. 본 연구에서는 K공사의 평균 최종학력보다 고학력자가 설문에 응하였고, 다소 많은 본사 근무자가 설문에 응했다고 볼 수 있다. 이것은 본사 근무여부에 따른 정보보안 스트레스 차이를 분석하고자 하는 본 연구의 목적에 따른 것이다.

다음으로 설문대상의 근무분야를 살펴보면 일반 사무직 종사자가 162명(67.3%), ICT보안업무 종사자가 78명(32.7%)을 차지하였으며, 회사 내 직위를 살펴보면 간부가 98명(40.9%), 일반직원이 142명(59.1%)을 차지하였다. 설문대상의 근무분야 및 직위는 다음 <표 4-4>와 같다.

<표 4-4> 조사대상의 근무분야 및 직위

근무분야	빈 도	비율(%)	직위	빈 도	비율(%)
사무	162	67.3	간부	98	40.9
ICT	78	32.7	직원	142	59.1
합계	240	100	합계	240	100

이는 K공사의 임직원 통계와는 다소 상이한 것으로 실제로 일반 사무직 종사자는 32.0%, ICT보안업무 종사자는 5.3%로 구성되어 있고, 회사 내 간부는 24.7%, 일반직원은 75.3%로 구성되어 있다. 이것은 일반 사무직 종사자와 ICT보안업무 종사자 사이에 보안 스트레스의 차이 및 간부와 일반직원 사이에 보안 스트레스의 차이를 분석하고자 하는 본 연구의 목적에 따른 것이다.

제 2 절 척도의 신뢰성과 타당성 검증

1. 신뢰성 분석

측정 변수 분석의 기초단계로 본 연구 설문조사에 사용된 문항들의 신뢰성 분석을 실시하였다. 신뢰성(Reliability)이란 유사한 측정도구 혹은 동일한 측정 도구를 사용하여 동일한 개념을 반복 측정했을 때 일관성 있는 결과를 얻는 것을 말한다. 본 연구모형에서는 사용된 요인들을 동일한 개념으로 측정하기 위해 다항목이 이용되었으므로 동일한 측정을 위한 항목간의 평균적인 관계를 Cronbach's Alpha계수에 의한 내적 일관성 분석을 실시하였으며 분석결과는 <표 4-5>와 같다.

신뢰성 분석에는 Cronbach's Alpha계수가 가장 널리 사용되며 Nunnally (1978)에 의하면, Cronbach's Alpha계수 값이 0.6이상이면 측정도구의 신뢰성이 확보된 것으로 볼 수 있다. 한편, Hair(1998)는 Cronbach's Alpha값이 0.7이상이면 설문의 신뢰성이 높다고 볼 수 있다고 하였으며, Boudreau(2001)은 엄격한 기준을 적용하여 통계분석을 위한 측정도구의 신뢰성을 0.8이상으로 제시하기도 하였다.

본 연구의 측정항목들의 신뢰성은 독립변수인 개인적 요인인 보안관심도 0.730, 회사환경 요인인 회사 보안 전략신뢰도 0.741, 회사 보안 교육수준 0.734, 종속변수인 기술적 보안 스트레스 0.760, 관리적 보안 스트레스 0.786, 물리적 보안 스트레스 0.724로 모두 0.7이상으로 분석되었다. 따라서 Cronbach's Alpha계수 값을 기준으로 볼 때, 본 연구의 측정도구는 높은 신뢰성을 확보한 것으로 볼 수 있다.

<표 4-5> 내적일관성법에 의한 문항분석

독립변수			종속변수		
변 수	항 목	항목제거시α	변 수	항 목	항목제거시α
보안 관심도 (α= 0.730)	1	0.721	기술적 스트레스 (α= 0.760)	1	0.702
	2	0.701		2	0.687
	3	0.698		3	0.700
	4	0.710		4	0.720
	5	0.762		5	0.771
전략 신뢰도 (α= 0.741)	1	0.694	관리적 스트레스 (α= 0.786)	1	0.796
	2	0.760		2	0.730
	3	0.711		3	0.749
	4	0.723		4	0.740
	5	0.639		5	0.751
교육수준 (α= 0.734)	1	0.724	물리적 스트레스 (α= 0.724)	1	0.702
	2	0.712		2	0.741
	3	0.705		3	0.713
	4	0.697		4	0.699
	5	0.725		5	0.705

2. 타당성 분석

본 연구의 측정변수에 타당성을 알아보기 위하여 설문조사에 사용된 문항들의 요인분석을 실시하였다. 타당성(Validity)이란 연구 도구가 실제 측정하고자 하는 연구 목적에 어느 정도로 부합하는지를 평가하는 개념이다. 요인분석에 의한 타당성 분석은 어떤 개념에 대하여 여러 가지

의 측정항목들을 이용하여 측정을 실시한 후, 각 항목들에 의한 측정치들의 요인을 분석하였을 때, 그 결과로 나온 요인들이 원래 의도한 개념을 대표할 수 있는가를 평가하는 것이다. 따라서, 하나의 요인 내에 묶여진 항목들은 개념을 측정한 것으로 간주할 수 있고, 각 요인은 서로 상이한 개념이라고 판단할 수 있다. 즉 요인내의 항목들은 집중타당성에 해당되며, 요인 간에는 판별타당성이 적용된다고 볼 수 있다.

<표 4-6> 요인분석 결과 (독립변수)

문 항		성 분		
		요 인1	요 인2	요인3
보안 관심도	1	0.197	0.835	0.248
	2	0.101	0.893	0.256
	3	0.188	0.780	0.124
	4	0.179	0.795	0.245
	5	0.123	0.755	
전략신뢰도	1	0.178	0.256	0.796
	2	0.145	0.357	0.845
	3	0.245	0.258	0.863
	4	0.301	0.342	0.794
	5	0.245	0.123	0.754
교육수준	1	0.687	0.350	0.146
	2	0.745	0.238	0.287
	3	0.834	0.382	0.366
	4	0.844	0.120	0.178
	5	0.787	0.265	0.197

본 연구에서는 측정변수의 구조적 개념을 독립변수, 종속변수로 나누어 요인분석을 실시하여 단일차원성을 확인하였다. 요인분석은 Kaiser정규화가 있는 베리맥스를 선택하여 회전하였으며 주성분분석을 활용하였다. 베리맥스 회전방법은 직각회전의 방법 중 하나로 요인행렬의 열분산

합계를 최대화함으로써 열을 단순화하는 방식이다. 이 방법은 각각의 항목들 간의 상관관계가 높은 것끼리 묶어서 하나의 요인을 형성하고 형성된 그룹간에 상호 독립적인 개념을 갖도록 하는 것이다. 요인 선정 기준은 요인 적재값이 0.4이상인 경우를 고려하였다. <표 4-6>은 독립변수에 대한 요인분석 결과이다. 모든 변수들의 각 항목들이 모두 각각의 요인으로 묶였으며 독립변수의 측정변수들 간에 내적 타당성이 확보된 것으로 나타났다.

아래의 <표 4-7>은 종속변수에 대한 요인분석 결과이다. 종속변수들의 문항에 대한 회전된 성분행렬 결과 각 항목들이 모두 각각의 요인으로 묶였으며 측정변수들 간에 내적 타당성이 확보된 것으로 나타났다.

<표 4-7> 요인분석 결과(종속변수)

문 항		성 분		
		요 인1	요 인2	요인3
기술적 보안 스트레스	1	0.221	0.025	0.817
	2	0.252	0.270	0.911
	3	0.286	0.279	0.840
	4	0.274	0.254	0.734
	5	0.173	0.124	0.753
물리적 보안 스트레스	1	0.723	0.224	0.297
	2	0.741	0.223	0.266
	3	0.756	0.217	0.226
	4	0.755	0.234	0.234
	5	0.850	0.145	0.136
관리적 보안 스트레스	1	0.187	0.813	0.247
	2	0.175	0.784	0.233
	3	0.226	0.759	0.245
	4	0.224	0.781	0.215
	5	0.321	0.712	0.165

3. 상관관계 분석

측정변수들 간의 개략적인 관계를 알아보기 위하여 상관관계 분석을 실시하였다. 상관관계 분석(Correlation Analysis)이란 연구하고자 하는 변수들간의 관련성을 분석하기 위해서 사용된다. 즉, 하나의 변수가 다른 변수와 관련성이 있는지의 여부와 관련성이 있다면 어느 정도의 관련성을 보유하고 있는지를 알아보고자 할 때 사용되는 분석 방법이다. 일반적으로 상관관계가 ±0.3 이하로 낮을 경우 측정항목 모집단과의 상관관계가 낮아 설문문항으로 부적합하다.

<표 4-8>은 변수들 간의 상관관계 분석의 결과이다. 결과를 분석해 보면 전체 표본에 대한 독립변수(보안관심도/회사 보안 전략신뢰도/회사 보안 교육수준)와 종속변수(기술적/관리적/물리적 보안 스트레스)와의 상관관계는 부(-)의 상관관계를 나타냄을 알 수 있다.

<표 4-8> 측정항목과 측정항목 모집단간의 상관관계

변 수	1	2	3	4	5	6
1. 보안관심도	1					
2. 전략신뢰도	0.303*	1				
3. 보안 교육수준	0.310	0.371*	1			
4. 기술적 보안 스트레스	-0.379*	-0.425*	-0.417*	1		
5. 관리적 보안 스트레스	-0.452**	-0.485**	-0.394**	0.352*	1	
6. 물리적 보안 스트레스	-0.284	-0.326*	-0.314	0.312*	0.314*	1

*p<.05, **p<.01

제 3 절 가설검증

가설 1. 조직 구성원의 특성은 기술적 보안 스트레스에 영향을 미칠 것이다.
1-1. 보안관심도가 높을수록 기술적 스트레스에 부(-) 영향을 미칠 것이다.
1-2. 전략신뢰도가 높을수록 기술적 스트레스에 부(-) 영향을 미칠 것이다.
1-3. 보안교육수준이 높을수록 기술적 스트레스에 부(-) 영향을 미칠 것이다.
1-4. 보안업무 담당 여부는 기술적 스트레스에 부(-) 영향을 미칠 것이다.
1-5. 회사 내 간부 여부는 기술적 스트레스에 부(-) 영향을 미칠 것이다.
1-6. 본사 근무 여부는 기술적 스트레스에 부(-) 영향을 미칠 것이다.

회귀분석(Regression Analysis)은 한 개 또는 그 이상의 독립변수들과 한 개의 종속변수의 관계를 파악하기 위한 분석기법이다. 본 연구에서는 가설 1을 검증하기 위하여 인구통계학적 특성을 통제변수(연령/성별/학력)로 정하고, 6개의 독립변수들과 종속변수(기술적 보안 스트레스)의 관계를 분석하는 기법인 다중회귀분석을 실시하였다. 결과 분석 시 R^2 값을 통하여 독립변수 요인이 종속변수를 어느 정도 설명하는지 알아보고, 변수별 표준화 계수와 유의확률을 중심으로 중속변수와 독립변수 간의 관계를 분석하였다. 다중회귀분석을 실시한 결과는 <표 4-9>와 같다.

분석결과 회귀모형의 설명력은 37.9%이고, 회귀식은 통계적으로 유의미한 것으로 분석되었다.(F=18.256, p=0.001) 개인적 요인 1개, 회사환경 요인 2개, 직무특성 요인 2개가 기술적 보안 스트레스에 유의미한 부(-)의 영향을 미치는 것으로 나타났으므로 가설 1은 일부채택 하였다.

<표 4-9>을 보면, 개인적 요인인 보안관심도가 높아지면 기술적 보안 스트레스는 0.256 낮아지는 것으로 나타났다. 회사환경 요인인 회사 보안

<표4-9> 개인적, 회사환경, 직무특성 요인이 기술적 보안 스트레스에 미치는 영향

구분		비표준화계수		표준화 계수β	유의 확률	수정된 R^2
		β	표준 오차			
상 수		3.060	0.667		0.070	
통제변수	연령	0.064	0.015	0.075	0.001**	
	성별	0.240	0.161	0.254	0.137	
	학력	-0.057	0.159	-0.067	0.722	
독립변수	보안관심도	-0.242	0.223	-0.256	0.036*	0.379
	전략신뢰도	-0.166	0.154	-0.174	0.022*	
	교육수준	-0.030	0.143	-0.055	0.032*	
	근무분야	-0.244	0.216	-0.263	0.018*	
	직위	-0.189	0.131	-0.172	0.015*	
	근무지	0.018	0.089	0.042	0.282	

*p<.05, **p<.01

전략신뢰도가 높아지면 기술적 보안 스트레스는 0.154 낮아지고, 회사 교육수준이 높아지면 기술적 보안 스트레스는 0.055 낮아지는 것으로 나타났다. 이는 앞서 보았던 선행연구들(김종기 등 2006; 박철주 등, 2012)과 동일한 결과를 갖는다고 할 수 있다.

직무특성 요인인 보안업무 담당 여부(근무분야)를 분석한 결과 ICT 보안업무 종사자는 일반 사무직 종사자보다 기술적 보안 스트레스가 0.263 더 낮은 것으로 나타났다. 보안업무 담당 여부는 기술적 보안 스트레스에 가장 큰 영향력(0.263)을 미치는 것으로 분석되었으며, ICT보안

업무 종사자가 더 많은 기술적 지식을 가지고 있기 때문에, 일반 사무직 종사자보다는 기술적 보안 스트레스가 낮은 것으로 추측된다. 특히 보안 관심도의 영향력(0.256)과 보안업무 담당여부의 영향력(0.263)은 기술적 보안 스트레스에 중요한 요인이므로 조직구성원의 스트레스를 최소화하기 위해 ICT보안업무 종사자는 좀 더 쉽고 편리한 시스템 및 정책 수립에 최선을 다해야 할 것이다.

회사 내 직위 측면에서 간부는 일반직원보다 기술적 보안 스트레스가 0.172 더 낮은 것으로 나타났다. 여기서 흥미로운 사실은 통제변수에서 연령이 높아질수록 기술적 보안 스트레스가 0.075 높아지는 것으로 나타났는데, 회사 내 간부여부는 정반대로 나타났다는 것이다. 평균적으로 간부가 일반직원보다 연령이 높기 때문에 직위 요인과 연령 요인이 동일한 영향력을 미칠 것으로 예상할 수 있으나, 본 연구에서는 반대의 결과를 얻었다. 이는 K공사 간부 승진 요건은 근속년수가 아닌 승진시험 합격여부이기 때문에 간부라고 해서 무조건 연령이 높은 것은 아니다. 2000년 이후 공기업 인력채용이 늘어났고, 그에 따라 자연적으로 젊은 직원의 승진이 늘어나 연령과 직위 요인이 동일하게 정(+)의 영향력을 미치지 않은 것으로 추측된다. 간부는 기술적으로 어려움이 따르고 불편함이 있더라도 회사측면에 보안의 중요성을 인식하고 적극적으로 정보보안 활동을 수행하여 기술적 보안 스트레스가 직원보다는 낮은 것으로 생각할 수 있다.

반면에 본사 근무 여부는 통계적으로 기술적 보안 스트레스에 유의한 영향을 미치지 않는 것으로 나타났다. 이것은 본사와 사업소 간 보안기술, 소프트웨어, 응용프로그램 등 정보보안의 기술적 요소가 동일하기 때문에 차이가 없었던 걸로 예상된다. 즉, 동일한 기술적 환경에서 근무하는 것은 기술적 보안 스트레스에 영향을 미치지 않는 것이다. ICT보안

업무 담당자는 이 결과를 주목하여, 본사와 사업소간 정보보안 기술적 요소에 차이가 발생하지 않도록 주기적으로 점검할 필요가 있다.

가설 2. 조직 구성원의 특성은 관리적 보안 스트레스에 영향을 미칠 것이다.
2-1. 보안관심도가 높을수록 관리적 스트레스에 부(-) 영향을 미칠 것이다.
2-2. 전략신뢰도가 높을수록 관리적 스트레스에 부(-) 영향을 미칠 것이다.
2-3. 보안교육수준이 높을수록 관리적 스트레스에 부(-) 영향을 미칠 것이다.
2-4. 보안업무 담당 여부는 관리적 스트레스에 부(-) 영향을 미칠 것이다.
2-5. 회사 내 간부 여부는 관리적 스트레스에 부(-) 영향을 미칠 것이다.
2-6. 본사 근무 여부는 관리적 스트레스에 부(-) 영향을 미칠 것이다.

가설 2를 검증하기 위하여 다중회귀분석을 실시한 결과는 <표 4-10>과 같다. 분석결과 회귀모형의 설명력은 38.0%이고, 회귀식은 통계적으로 유의미한 것으로 분석되었다.(F=16.208, p=0.000) 개인적 요인 1개, 회사환경 요인 2개, 직무특성 요인 3개가 관리적 보안 스트레스에 유의미한 부(-)의 영향을 미치는 것으로 나타났으므로 가설 2는 채택 하였다.

<표 4-10>을 보면, 개인적 요인인 보안관심도가 높아지면 기술적 보안 스트레스는 0.040 낮아지는 것으로 나타났다. 또한 회사환경 요인인 회사 보안 전략신뢰도가 높아지면 관리적 보안 스트레스는 0.173 낮아지는 것으로 나타났다. 이는 앞서 보았던 선행연구들(정구헌 등, 2011; 이장호, 2013)과 동일한 결과를 갖는다고 할 수 있다.

회사 보안 교육수준이 높아지면 관리적 보안 스트레스는 0.345 낮아지는 것으로 나타났다. 예전에는 강제적으로 정보보안 교육을 수강하도록 하여 이에 따른 스트레스가 발생하였지만, 최근 들어 잇따라 발생하는 보안 침해사고를 통해 정보보안의 중요성에 대한 관심이 날로 높아지

<표 4-10> 개인적, 회사환경, 직무특성 요인이 관리적 보안 스트레스에 미치는 영향

구분		비표준화계수		표준화 계수β	유의 확률	수정된 R^2
		β	표준 오차			
상 수		3.058	0.748		0.000**	0.380
통제변수	연령	0.026	0.016	0.192	0.109	
	성별	-0.553	0.178	-0.309	0.002**	
	학력	0.139	0.176	0.080	0.428	
독립변수	보안관심도	0.070	0.136	-0.040	0.028*	
	전략신뢰도	0.269	0.170	-0.173	0.016*	
	교육수준	0.512	0.158	-0.345	0.001**	
	근무분야	0.069	0.129	-0.042	0.042*	
	직위	0.015	0.145	-0.014	0.040*	
	근무지	0.184	0.198	-0.156	0.030*	

*p<.05, **p<.01

는 추세를 반영한 것이라 하겠다. 이러한 상황 속에서 정보보안 교육은 강제적 수단에 의한 스트레스가 아닌, 보안 침해사고를 예방할 수 있는 대책으로서 자리를 잡고 있는 것이다. 특히 회사 보안 교육수준은 관리적 보안 스트레스에 가장 큰 영향력(0.345)을 미치는 것으로 분석되었으며, 조직구성원에 대한 회사의 정보보안 교육 정책의 중요성을 다시 한 번 확인할 수 있었다. ICT보안업무 종사자는 조직구성원의 관리적 보안 스트레스에 가장 큰 영향력을 미치는 요인인 회사 보안 교육수준을 높이기 위해 보다 쉽고, 마음에 와 닿을 수 있는 사례 중심의 보안 교육과정을 만들 수 있도록 노력할 필요가 있다.

직무특성 요인인 근무분야 측면에서는 ICT보안업무 종사자는 일반 사무직 종사자보다 관리적 보안 스트레스가 0.042 더 낮은 것으로 나타났다. 회사 내 직위 측면에서 간부는 일반직원보다 관리적 보안 스트레스가 0.014 더 낮은 것으로 나타났다.

본사 근무여부 측면에서 본사에 근무하는 직원은 사업소인 사업본부에서 근무하는 직원보다 관리적 보안 스트레스가 0.156 더 낮은 것으로 나타났다. 이것은 본사 근무여부가 기술적 보안 스트레스에서는 통계적으로 유의한 영향을 미치지 않는 것과는 다른 결과이다. 대부분의 중요 회사 데이터가 본사에 위치하므로 본사 측면의 강도 높은 관리적 보안 시스템이 정착되어 본사 근무 직원들이 체감하는 스트레스는 적은 것으로 추측된다. 특히 국정원, 감사원, 지식경제부 등 대외기관의 불시점검 등 상시 준비되어있는 본사 관리체계가 사업소 관리체계보다 효율적으로 운영되고 있다는 것을 설명한다.

가설 3. 조직 구성원의 특성은 물리적 보안 스트레스에 영향을 미칠 것이다.
3-1. 보안관심도가 높을수록 물리적 스트레스에 부(-) 영향을 미칠 것이다.
3-2. 전략신뢰도가 높을수록 물리적 스트레스에 부(-) 영향을 미칠 것이다.
3-3. 보안교육수준이 높을수록 물리적 스트레스에 부(-) 영향을 미칠 것이다.
3-4. 보안업무 담당 여부는 물리적 스트레스에 부(-) 영향을 미칠 것이다.
3-5. 회사 내 간부 여부는 물리적 스트레스에 부(-) 영향을 미칠 것이다.
3-6. 본사 근무 여부는 물리적 스트레스에 부(-) 영향을 미칠 것이다.

가설 3을 검증하기 위하여 다중회귀분석을 실시한 결과는 <표 4-11>과 같다. 분석결과 회귀모형의 설명력은 31.1%이고, 회귀식은 통계적으로 유의미한 것으로 분석되었다.(F=15.803, p=0.000) 회사환경 요인 1개, 직무특성 요인 2개가 물리적 보안 스트레스에 유의미한 부(-)의 영향을 미

<표 4-11> 개인적, 회사환경, 직무특성 요인이 물리적 보안 스트레스에 미치는 영향

구분		비표준화계수		표준화 계수β	유의 확률	수정된 R^2
		β	표준 오차			
상 수		3.804	0.647		0.000**	0.309
통제변수	연령	0.031	0.014	0.024	0.028	
	성별	-0.078	0.154	-0.190	0.611	
	학력	-0.265	0.152	-0.216	0.182	
독립변수	보안관심도	-0.117	0.118	-0.092	0.321	
	전략신뢰도	-0.269	0.147	-0.275	0.013*	
	교육수준	-0.026	0.137	-0.048	0.252	
	근무분야	-0.157	0.111	-0.169	0.016*	
	직위	-0.110	0.126	-0.105	0.025*	
	근무지	-0.257	0.085	-0.210	0.382	

*p<.05, **p<.01

치는 것으로 나타났으므로 가설 3은 일부채택 하였다.

<표 4-11>을 보면 개인적 요인인 보안관심도와 회사환경 요인인 회사 보안 교육수준은 선행연구의 결과들(이신권 2012; 신호영, 2013)과는 다르게 통계적으로 물리적 보안 스트레스에 유의한 영향을 미치지 않는 것으로 나타났다. 이것은 보안관심도 및 회사 보안 교육수준이 기술적, 관리적 보안 스트레스에 통계적으로 유의한 영향을 미치는 것과도 다른 결과이다.

개인적인 지식이 높고, 관심이 높다하더라도 PC, 건물 등에 물리적

접근, 접속 차단의 통제로 인한 보안 스트레스 체감은 피할 수 없다는 것을 의미한다. 또한 보안 교육 프로그램의 충실도 및 신뢰도가 물리적 보안 스트레스를 줄일 수 있을 정도로 높지 않음을 의미한다. 향후 ICT 보안업무 종사자는 이 부분을 반영하여 정보보안 교육 프로그램을 개선할 필요가 있다.

회사환경 요인인 회사 보안 전략신뢰도가 높아지면 물리적 보안 스트레스는 0.375 낮아지는 것으로 나타났다. 이는 앞서 보았던 선행연구들(이신권, 2012; 신호영, 2013)과 동일한 결과를 갖는다고 할 수 있다. 특히 회사 보안 전략신뢰도는 물리적 보안 스트레스에 가장 큰 영향력(0.375)을 미치는 것으로 분석되었다. 이는 회사 정보보안 전략상 꼭 필요하다 인정하는 경우는 과다한 정보보안 업무프로세스라 하더라도 조직구성원들이 체감하는 물리적 보안 스트레스는 줄어들 수 있다는 것을 의미한다고 볼 수 있다.

직무특성 요인 측면에서 ICT보안업무 종사자는 일반 사무직 종사자보다 관리적 보안 스트레스가 0.189 더 낮은 것으로 나타났다. 결국 보안업무 담당 여부는 모든 분야의 정보보안 스트레스에 부(-)의 영향을 미치는 것으로 분석되었다. 회사 내 직위 측면에서 간부는 일반직원보다 물리적 보안 스트레스가 0.025 더 낮은 것으로 나타났다. 이것은 물리적 접근 및 접속 통제는 관리적 역할을 담당하는 간부보다 실무적 역할을 담당하는 일반 직원에게 더 큰 스트레스로 작용한다는 것을 의미한다.

본사 근무여부는 통계적으로 물리적 보안 스트레스에 유의한 영향을 미치지 않은 것으로 나타났다. 이것은 기술적 보안 요소와 마찬가지로 본사와 사업소간에 물리적 보안 요소가 동일하기 때문에 두 집단에 느끼는 물리적 보안 스트레스에 차이가 없었던 걸로 예상된다. 결국 본사 근무여부는 관리적 보안 스트레스에만 유의한 영향을 미치는 것으로 나타났다.

제 5 장 결론

제 1 절 연구결과의 요약

본 연구에서는 조직구성원들의 특성(보안관심도, 전략신뢰도, 교육수준, 보안업무 담당 여부, 간부 여부, 본사 근무여부)이 각 분야별 정보보안 스트레스(기술적, 관리적, 물리적)에 미치는 영향을 검증하였다. 이를 위해 정보보안 및 스트레스에 관한 개념적, 실증적 연구들을 살펴보고, 이를 토대로 정보보안 스트레스 요인들을 구분하고, 실증적 연구 모형을 통해 가설을 설정하고 검증해보았다.

가설의 검증을 위해 K공사의 본사 및 3개 사업본부를 대상으로 설문조사를 하여 240개의 유효한 자료를 확보하였다. 분석의 방법으로 빈도분석, 신뢰도 분석, 요인 분석, 상관관계 분석 및 다중회귀분석을 실시하였다. 연구모형에 대한 가설 검증 결과는 다음 <표 5-1>과 같이, 총 3개 중 채택 1개, 일부 채택 2개 였다. 이에 따른 본 연구의 분석 결과는 아래와 같이 요약할 수 있다.

첫째, 조직구성원의 특성관련 총 6개 요인 중 5개가 기술적 보안 스트레스에 통계적으로 유의미한 부(-)의 영향을 미치는 것으로 나타났다. 세부적으로 살펴보면 본사 근무 여부는 제외하고, 보안관심도, 회사 보안 전략신뢰도, 회사 보안 교육수준, 보안업무 담당 여부, 간부 여부가 부(-)의 영향을 미쳤다. ICT보안업무 종사자와 간부는 일반 사무직 종사자와 일반직원들이 체감하는 기술적 보안 스트레스에 차이가 있음을 인식하고, 향후 최신 보안기술, 소프트웨어, 응용 프로그램 도입 시 좀 더 쉽고, 편리하게 운영·관리될 수 있도록 방안을 수립해야 할 것이다.

<표 5-1> 연구가설 채택 여부

가설		채택여부
가설 1.	조직 구성원의 특성은 기술적 스트레스에 영향을 미칠 것이다.	일부채택
1-1.	보안관심도가 높을수록 기술적 스트레스에 부(-) 영향을 미칠 것이다.	채택
1-2.	전략신뢰도가 높을수록 기술적 스트레스에 부(-) 영향을 미칠 것이다.	채택
1-3.	보안교육수준이 높을수록 기술적 스트레스에 부(-) 영향을 미칠 것이다.	채택
1-4.	보안업무담당여부는 기술적 스트레스에 부(-) 영향을 미칠 것이다.	채택
1-5.	회사 내 간부 여부는 기술적 스트레스에 부(-) 영향을 미칠 것이다.	채택
1-6.	본사 근무여부는 기술적 스트레스에 부(-) 영향을 미칠 것이다.	불채택
가설 2.	조직 구성원의 특성은 관리적 스트레스에 영향을 미칠 것이다.	채택
2-1.	보안관심도가 높을수록 관리적 스트레스에 부(-) 영향을 미칠 것이다.	채택
2-2.	전략신뢰도가 높을수록 관리적 스트레스에 부(-) 영향을 미칠 것이다.	채택
2-3.	보안교육수준이 높을수록 관리적 스트레스에 부(-) 영향을 미칠 것이다.	채택
2-4.	보안업무담당여부는 관리적 스트레스에 부(-) 영향을 미칠 것이다.	채택
2-5.	회사 내 간부 여부는 관리적 스트레스에 부(-) 영향을 미칠 것이다.	채택
2-6.	본사 근무여부는 관리적 스트레스에 부(-) 영향을 미칠 것이다.	채택
가설 3.	조직 구성원의 특성은 물리적 스트레스에 영향을 미칠 것이다.	일부채택
3-1.	보안관심도가 높을수록 물리적 스트레스에 부(-) 영향을 미칠 것이다.	불채택
3-2.	전략신뢰도가 높을수록 물리적 스트레스에 부(-) 영향을 미칠 것이다.	채택
3-3.	보안교육수준이 높을수록 물리적 스트레스에 부(-) 영향을 미칠 것이다.	불채택
3-4.	보안업무담당여부는 물리적 스트레스에 부(-) 영향을 미칠 것이다.	채택
3-5.	회사 내 간부 여부는 물리적 스트레스에 부(-) 영향을 미칠 것이다.	채택
3-6.	본사 근무여부는 물리적 스트레스에 부(-) 영향을 미칠 것이다.	불채택

둘째, 조직구성원의 특성관련 총 6개 요인 중 6개 모두가 관리적 보안 스트레스에 통계적으로 유의미한 부(-)의 영향을 미치는 것으로 나타

났다. 이것은 개인적 요인, 회사환경 요인, 직무특성 요인 등 모든 요인들이 조직구성원들이 체감하는 스트레스를 낮춘다는 의미이다. 국정원, 지식경제부 등에 의한 정보보안 지시사항을 접수 후 보안 이행 계획 및 정책을 수립하는 과정에서 관리적 보안 스트레스 유발을 최소화하기 위해 일방향적 정책 수립이 아닌, ICT보안업무 종사자와 일반 사무직 종사자, 간부와 일반직원, 본사 근무자와 사업소 근무자 간 소통을 통한 양방향적 정책 수립이 필요함을 의미한다.

셋째, 조직구성원의 특성관련 총 6개 요인 중 3개가 물리적 보안 스트레스에 통계적으로 유의미한 부(-)의 영향을 미치는 것으로 나타났다. 세부적으로 살펴보면 보안관심도, 회사 보안 교육 수준, 본사 근무 등 3개 요인은 제외하고, 회사 보안 전략신뢰도, 보안업무 담당 여부, 간부 여부가 부(-)의 영향을 미쳤다. 각 분야별 정보보안 스트레스의 회귀모형에 대한 설명력을 비교해보면 관리적 보안 스트레스(38.0%) > 기술적 보안 스트레스(37.9%) > 물리적 보안 스트레스(30.9%)로 물리적 보안 스트레스가 가장 낮음을 알 수 있다. 물리적 보안은 PC, 건물 등에 물리적 접근, 접속 차단의 통제를 통한 극단적인 정보보안 요소이기 때문에 다른 보안 요소보다 기본적으로 스트레스가 높다. ICT보안업무 종사자와 간부는 물리적 보안의 특수성을 고려하여 스트레스를 줄이기 위한 추가적 노력이 필요하다.

이와 같은 결론을 종합해 볼 때 개인적 요인, 회사환경 요인, 직무특성 요인들은 정도의 차이는 있지만 대부분 정보보안 스트레스에 긴밀한 영향을 미치는 것으로 분석되었다. 특히, 회사 보안 전략신뢰도, 보안업무 담당여부, 간부 여부 등 3개 요인은 모든 정보보안 스트레스(기술적, 관리적, 물리적)에 부(-)의 영향을 미치는 것으로 나타났다.

제 2 절 연구의 시사점 및 한계점

1. 연구의 시사점

최근 들어 정보보안 사고가 끊임없이 발생하고 있어 이와 관련한 그동안의 연구들은 정보보안 성과에 집중되어 왔다. 정보보안 피해를 경험한 기업들은 보안 강화를 위해 노력하고 있지만, 다른 측면에서 바라보면 이러한 노력은 조직구성원들이 느끼는 스트레스의 증가 요인으로 작용할 수 있다. 본 연구는 정보보안 성과를 높이기 위한 정보보안 강화, 통제 및 그 활동들이 실제로 조직구성원들에게 얼마나 불편함을 주고 있는지 각 분야별 정보보안 스트레스를 통해 분석한다는 것에 그 의미가 있다. 향후 효율적인 정보보안 강화 방안을 수립함에 있어 구성원들의 스트레스를 최소화하려면 고려해야 할 항목들이 어떤 것인지 어느 정도 제시할 수 있다고 생각된다.

본 연구를 통해 K공사 조직구성원들이 체감하는 정보보안 스트레스에 영향을 미치는 요인을 분석하여, 조직구성원들이 체감하는 정보보안 스트레스를 최소화할 수 있는 방안 제시에 필요한 유의미한 분석 결과를 얻었다. 따라서, 정보보안 대책 수립 초기 단계에서부터 사후 관리 감독하는 단계까지 다음과 같은 방안들을 제시하고자 한다.

첫째, 회사 보안 전략신뢰도 향상 방안을 도출해야한다. 회사 보안 전략신뢰도는 모든 분야의 정보보안 스트레스에 부(-)의 영향을 미친다는 분석 결과를 얻었다. 회사에서 보안 정책 수립 시 업무의 생산성과 보안 준수간의 상충관계를 고려한 절충안을 마련하여 보안 준수가 생산성을 하락시킨다는 부정적 인식을 전환시킬 필요가 있다. 또한 정보보안 참해

로 인해 회사가 받게 되는 잠재적 피해와 이러한 영향이 조직에 미칠 영향을 함께 공유함으로써 조직구성원들 스스로 보안에 대한 중요성을 인식하도록 할 뿐만 아니라 전략신뢰도로 높일 수 있는 기회로 삼아야 할 것이다.

이제부터라도 국가정보보호백서를 통해 살펴보았듯이 회사는 매월 단위로 침해사고 접수처리 건수를 공개하여야 한다. 이것은 회사 조직구성원들을 위해 적극적으로 보안 사고에 대처하고 있다는 것을 보여줘 전략신뢰도를 높일 뿐만 아니라 구성원들 개개인의 보안관심도 향상에도 기여할 것이다. 침해사고를 공개함과 동시에 조직구성원들의 보안활동 참여에 대한 적절한 보상 제도를 만들어야 할 것이다. 정보보안의 통제로 인해 스트레스가 유발되므로 보상을 통한 상충 작용이 필요한 때이다. 정보보안을 통해 그 동안 징계 받은 직원은 많아도 칭찬을 받은 사람은 손에 꼽을 정도이다. 더 많은 보안 기술을 습득한 ICT보안업무 종사자는 일반 사무직 직원들에게 보안 정책 준수 시 적절한 보상을 통해 관심도를 높일 수 있다. 이러한 정보보안 칭찬·보상 문화가 정착이 된다면 직원들의 조직 몰입을 가져올 수 있을 것이다. 이러한 조직문화는 가치관, 믿음을 가져옴으로써 조직체계의 안정성 및 신뢰도를 높이는 데 기여할 것이다.

또한, 정보보안 전문가 양성을 통해 회사 보안 전략신뢰도 향상에 기여해야한다. 정부 조직 개편, 새로운 CEO 취임 등 현안사항 발생 시마다 되풀이되는 조직의 잦은 변화에 따른 보안담당자의 빈번한 인사이동은 인력공백 및 인력관리의 허점 발생이라는 측면에서 조직구성원에게 불안감을 조성할 수 있으므로 각별히 유의해야 할 것이다.

둘째, 물리적 보안 스트레스를 최소화하는 방안을 도출해야 한다. 물리적 보안 특성 상 조직구성원이 체감하는 스트레스는 가장 높으나, 본

연구에서는 다른 스트레스에 비해 회귀모형에 대한 설명력이 다소 낮았다. 우선 물리적 보안의 세부 측정항목에 대한 방안을 제시하고자 한다.

가장 많은 스트레스를 초래하는 항목 중 하나인 보안USB를 통한 통제는 클라우드 기술이 대안이 될 수 있다. 클라우드(Cloud)란 복잡하고 번거로운 일들을 더 이상 지상(PC)에서 처리하지 않고 구름 위(중앙서버)로 올려 보내 필요할 때마다 중앙서버와 연결해 쓴다는 의미이다. 개인별로 가상의 하드디스크를 제공하여 자신의 데이터를 중앙서버에 올려놓고 출장 시에도 회사PC에서 내 자리처럼 데이터를 사용할 수 있는 최신 기술이다. 클라우드 서비스를 적용하면 국내외 출장, 인사이동 등 따른 이동시 보안USB에 자료를 반출하는 불편함을 대폭 완화할 수 있다.

무선랜(와이파이[6]) 접속 차단에 의한 통제는 모바일 플랫폼 기술이 대안이 될 수 있다. 현재 우리나라 스마트폰 이용자는 2,500만명으로 전체 인구의 50%는 스마트폰을 이용하고 있다.(방송통신위원회, 2012) 회사 내부적으로도 스마트폰 이용자가 급속도로 증가하고 있는 추세 속에서 시대에 뒤떨어진 무선랜 접속 차단은 업무에 큰 불편을 초래하고 있다. 모바일 플랫폼은 모바일 엔진, 정보보안 인증서버 및 agent 등을 포괄하는 기술이다. 보안 agent가 설치된 모바일 기기가 모바일 인증서버로 인증을 요청하면 모바일 인증서버는 사내 통합인증서버와 연계하여 접속 승인여부를 판단하게 된다. 이러한 최신 기술 도입은 무선랜 접속 차단에 의한 물리적 보안 스트레스 완화에 큰 도움을 줄 것이다.

셋째, ICT보안업무 종사자는 일반 사무직 종사자가 체감하는 보안 스트레스에 차이가 있음을 인식해야 한다. 간부 또한 일반직원과 체감하는 보안 스트레스에 차이가 있음을 인식해야 한다. 보안업무 담당 여부

6) 와이파이(Wi-Fi)는 Wireless Fidelity의 약자로 무선 접속 장치(AP: Access Point)가 설치된 곳에서 전파나 적외선 전송 방식을 이용하여 일정 거리 안에서 무선 인터넷을 할 수 있는 근거리 통신망을 칭하는 기술이다.

와 간부 여부는 모든 분야의 정보보안 스트레스에 부(-)의 영향을 미치는 것으로 나타났다. 보안정책을 수립하는 직원과 실제로 그 보안정책을 따르는 사용자로서의 일반 사무직 종사자의 스트레스는 차이가 생길 수 밖에 없고, 보안업무 종사자는 자기도 모르는 사이에 그 차이를 간과하게 된다. 본 연구를 통해 밝혀졌듯이, ICT보안업무 종사자는 항상 합리적이고 효율적인 보안기술 및 보안시스템 도입 할 수 있도록 방향을 제시하도록 노력해야한다. 최신 보안기술이나 솔루션 도입만으로 기업이 당면한 보안 문제를 해결할 수는 없다. 아무리 좋은 보안기술이나, 제품을 가지고 있다고 하더라도 이를 뒷받침할만한 정책이나 일반 사무직 종사자 쉽게 이해할 수 있도록 해석해주는 역할을 하는 ICT보안업무 종사자가 없다면 결국 투자비용만 낭비하고 조직구성원에서 스트레스만 초래하는 결과를 낳을 것이다.

또한, 간부들은 정보보안 절차를 스스로 이행하도록 더욱 노력해야한다. 보안USB, 내PC지미키, 보안 프로그램 업데이트 등의 보안 이슈들을 자신이 해결하지 못할 경우 일반 직원들에게 시키는 경우가 비일비재하다. 간부로서 회사 보안 정책의 중요성을 이해는 하고 있지만, 그것을 실행으로 옮기지 못하고, 대리인(부하직원)을 통해 처리한다는 것은 용납될 수 없는 일이다.

2. 연구의 한계점

본 연구는 시간적, 공간적 한계점과 연구진행에서 오는 한계점을 내포하고 있는 관계로 향후 연구에서는 다음과 같은 사항들을 고려하여 연구를 진행해야 할 것이다.

첫째, K공사에 근무하고 있는 직원들을 대상으로 조사한 자료를 활용한 관계로 한정된 자료의 보편성, 일반성을 확보하려고 노력하였으나, 우리나라 전체로 일반화하기에는 한계점을 지니고 있다. 특히 K공사의 특징 중 하나인 표본대상의 한계점도 존재한다. 남성 직원 비율이 높음, 40대 이상 직원 비율이 높음 등으로 인해 연구이론을 일반화하기에는 한계가 있다. 따라서 향후에는 정부, 기타 공공기간 및 민간기업 등 다양한 기관, 산업군에 근무하는 관계자들의 인식조사를 통해 자료의 일반화와 보편화를 확대하도록 해야 할 것이다.

둘째, 본 연구는 정보보안 스트레스에 영향을 미치는 요인으로 개인적 요인(보안관심도), 회사환경 요인(회사 보안 전략신뢰도, 회사 보안 교육수준), 직무특성 요인(근무분야, 직위, 근무지)로 구분하여 효과를 파악하고자 했지만, 정보보안 스트레스에 영향을 줄 수 있는 다른 다양한 변수들을 고려하지 못하였다. 향후에는 정보보안 스트레스에 영향을 미칠 수 있는 변수를 추가적으로 찾아내는 작업이 필요할 것으로 생각한다.

셋째, 본 연구에서 종속변수인 정보보안 스트레스는 기술적, 관리적, 물리적 3개의 분야로 구분되어 측정되어졌다. 각 분야별로 다시 한 번 세부적으로 살펴보면 다양한 항목들로 구분되어져 있다. 여러 항목들 중 어떤 항목들이 각 정보보안 분야의 대표성을 띄는지 향후에도 지속적으로 분류해나가야 할 것이다.

정보기술의 존재 목적은 인간의 문제를 해결해주고 인간의 삶의 질을 향상시키는 것이다. 조직구성원들이 이해할 수 있고, 스스로 긍정적으로 즐길 수 있는 전략을 통해 보안 스트레스를 예방, 정복, 그리고 적응할 수 있도록 관리해나가는 것이 필요하다. 따라서, 본 연구의 한계를 극복하여 정보보안 스트레스 요인을 추가적으로 명확하게 밝혀내는 성공적인 연구가 있기를 기대한다.

참고문헌

강성민・송은수. (2008). 전자상거래 기업환경에서의 시스템 사용자의 정보보안에 대한 연구.「전자무역연구」. 6(1): 1-37.

김영곤. (2010). 정보보안 거버넌스의 구성요소가 종업원의 보안 인식과 행위에 미치는 영향에 관한 연구.「한국항행학회」. 14(6): 935-950.

김종기・전진환・임호섭. (2006). 정보보안정책, 보안통제 및 사용자 특성이 정보보안효과에 미치는 영향: 컴퓨터 바이러스를 중심으로.「정보시스템연구」. 15(1): 145-168.

김현수・정해철. (1999). 정보보안 지표 개발에 관한 탐색적 연구.「국제학술대회」. 3(1): 119-127.

구자면. (2012). 정보보안체계 수립이 Multibusiness 기업 성과에 미치는 영향에 관한 연구: ICT Relatedness 관점에서. 경희대 대학원 박사학위 논문.

박광희・유화숙. (2003). 직무스트레스에 관한 문헌적 고찰.「대한가정학회지」. 41(6): 167-183.

박준형. (2008). 조직 특성에 따라 처벌과 윤리적 교육이 정보보안 효과에 미치는 영향. 서울대학교 대학원 석사학위논문.

박상서・박춘식. (2008). 조직내 정보시스템 보안 전략의 성공적 구현을 위한 정보시스템 보안 전략의 특성.「정보보안 논문지」. 8(3);101-106

박철주・임명성. (2012). 기술스트레스가 조직원 보안 인식과 조직성과에 미치는 영향에 관한 연구.「한국정보기술학회논문지」. 10(1): 97-110.

백민정. (2010). 정보윤리활동이 정보보안성과에 미치는 영향에 관한 연구. 단국대학교 경영대학원 박사학위 논문.

송영미. (2013). 조직 내 정보기술능력이 정보보안관리 동화에 미치는 영향 및 최고경영진의 주도와 정책기술간 조화의 조절효과에 관한 연구. 경북대학교 대학원 박사학위 논문.

신영진. (2004). 정보보호정책의 국제비교연구: 정책지표 개발과 전략적 우선순위 분석을 중심으로. 성균관대학교 대학원 박사학위 논문.

신호영. (2013). 스마트폰 이용자들의 정보보안 행위의도에 관한 실증연구. 영남대학교 대학원 박사학위 논문.

이은옥・김매자. (1974). 양털, Gel Pad 및 Sponge의 예방 및 치료효과에 관한 연구.「대한간호학회지」. 4(3): 93-104.

이신권. (2012). 공공기관 ICT보안 업무 종사자의 직무스트레스 결정 요인에 대한 실증 연구: 보안스트레스에 대한 제도적, 기술적, 문화적, 개인적 요인의 영향을 중심으로. 고려대학교 정보보호 대학원 석사학위 논문.

이선중・이미정. (2008). 정보보호 문화의 평가 지표에 관한 탐색적 연구.「정보화정책」. 15(3): 100-119.

이장호. (2013). IT보안업무 종사자의 직무스트레스와 직무태도 관계 분석; 직무만족과 조직몰입을 중심으로. 고려대학교 정보보호대학원 석사학위 논문.

이창환. (2011). 보안정책에 미치는 영향요인에 관한 연구. 경원대학교 대학원 박사학위 논문.

장세진. (2000). 스트레스. 건강통계자료 수집 및 측정의 표준화. 대한예방의학회.

장세진 등 17명. (2005). 우리나라 직장인 스트레스의 역학적 특성.

「예방의학회지」. 38(1): 71-81.

정구헌・정승렬. (2011). 정보보호 통제활동이 조직유효성에 미치는 영향: 정보활용의 조절효과를 중심으로.「지능정보연구」. 17(1): 77-90.

차경태 등 8명. (2008). 사무직 근로자들의 직무 스트레스와 피로.「대한산업의학회지」. 20(3): 182-192.

차인환. (2009). 정보보안에서의 인원보안 관리지표 개발을 위한 실증적 연구. 광운대학교 대학원 박사학위 논문.

탁진국. (2002). 직종에 따른 직무스트레스원과 직무스트레스에서의 차이.「한국심리학회지:건강」. 7(1): 125-141.

탁진국・이강숙・홍현숙. (2002). 사무직 직급에 따른 스트레스에 미치는 요인에서 차이에 관한 연구.「예방의학회지」. 35(2): 160-168.

홍기향. (2003). 정보보호 통제와 활동이 정보보호 성과에 미치는 영향에 관한 연구. 국민대학교 대학원 박사학위 논문.

국가정보원. (2013). 2013년 국가정보보호백서.

남길현・원동호. (2010). 정보시스템 보안론.

방송통신위원회. (2012). 유・무선 통계조사 보고서.

한국인터넷진흥원. (2011). 인터넷 침해사고 동향 및 분석원본.

한국정보보호진흥원. (2007). ISMS인증제도 소개.

한국전력공사. 보안업무 처리지침. (2012).

Boudreau, M. D. Gefen and D. Strauh. (2001). Validation in information systems research: A state of the art assessment. Mis Quarterly. 25(1): 1-16

Cannon W. B. (1929). Bodily changes in pain, hunger, fear and rage. Journal of Psychology. Vol. 25.

Goldberg, D. (1978). Manual of the General Health Questionare. Winsor;

NFER Publishing Co.

Hair, J. R. Anderson, R. Tatham and W. Black. (1998). Multivariate data analysis. Fifth Edition. Prentice Half International Inc.

Nunnally, J. C. (1978). Psychological Theory; McGraw Hill.

Solms R. (1998). Information security mannagement(1) : why information security is important. Informaio수 Management & Computer Security Vol. 6 Issue 4.

Wack, J. and L. Carnahan. (1989). Computer Viruses and Related Treats: A Management Guide. NIST SP 500-166, National Institute of Standards and Technology.

Abstract

Study on information security stress in Public Enterprise

Sung Min Ryu
Department of Public Administration
The Graduate School
Seoul National University

The purpose of this study is to analyze factors affecting information security stress to company staffs and propose ways to minimize stress, also to establish effective information security policy.

To accomplish this study, a survey on headquarter and 3 division office in K public Enterprise was conducted and 240 valid data were obtained. For data analysis, statistical analysis, factor analysis, reliability analysis, and multi regression analysis were made.

The results obtained on the study are as follows.

First, it shows that factors related to the characteristics of the company staffs of 5 of the total 6 were affecting technical security stress validly in statistics. In details, interest in security, reliability on company security strategy, level of security education, job related to information security and position status in company affected information security stress negatively, except working status in

headquarter, The staff working in ICT(Information Communication Technology) security field should recognize that the stress is different from stress of the staff working in normal office and develop a plan to make easy security technology, software and programme.

Second, it shows that factors related to the characteristics of the company staffs of 6 of the total 6 were affecting administrative security stress validly in statistics. This means that personal factor, company circumstance factor and job characteristics factor lower all kind of stress on company staffs. After receiving instructions from the government, the company should develop a effective plan communicating between company and all of the staff.

Third, it shows that factors related to the characteristics of the company staffs of 3 of the total 6 were affecting physical security stress validly in statistics. In details, reliability on company security strategy, job related to information security and position status in company affected information security stress negatively, except interest in security, level of security education and working status in headquarter. As it shows the explanatory power of the regression model, the explanatory power of physical information security stress is the lowest. Because physical security is related to blocking the access of PC and building, stress on physical security is higher than technical and administrative stress on information security. The staff working in ICT field need more effort to lower stress on physical security considering the particularity.

As a result, this study suggests the ways to lower stress on

information security. First of all, a plan should be developed to improve the reliability on company security strategy. The company should effort to change negative perceptions that security compliance decrease productivity. Second, a plan should be developed to lower the stress on physical information security. The company should try to lower the stress on physical security with the latest ICT. Third, the staff working in ICT field should realize the difference of stress between the staff working in normal office. They should introduce rational, effective and reasonable security technology and system. They should work as interpreter of high technology to staff working in office. And they should monitor to find out the factor of stress all the time, and look for the way to lower it.

keyword : information security, information protection, stress, ICT security, public enterprise, security regulation

student number : 2012-22781

설문지

* 본 조사의 내용은 통계법 제 13조에 의거하여 비밀이 보장되며 통계적 목적 이외에는 사용되지 않습니다.

안녕하십니까?

본 설문지는 서울대학교 행정대학원 석사학위 논문으로 「정보보안 스트레스 요인에 관한 연구」를 위한 실증조사를 위한 것입니다. 따라서 응답 자료는 순수하게 학문적 연구목적 이외에는 일체 사용되지 않으며 오직 통계적으로 처리되므로 익명성이 보장됩니다.

설문지의 문항들에 대해 귀하의 성의 있고 솔직한 응답을 부탁드립니다.

귀하의 응답은 연구목적으로만 사용되며 본 연구를 위해 매우 소중한 자료로서 좋은 연구결과를 얻기 위한 기초가 될 것입니다.

설문 작성에 응해주셔서 깊은 감사의 말씀 드립니다.

2013년 2월

지도교수 : 서울대학교 행정대학원 교수 우 지 숙
연 구 자 : 서울대학교 행정대학원 공기업정책학과 석사과정 유 승 민

연락처 : 010-9420-1190
이메일 : ryu2470@kepco.co.kr

※ 추신 : 저의 연구에 관심이 있으신 분께서는 이메일이나 전화로 연락을 주시면 빠른 시일 내에 연구결과를 보내드리겠습니다.

I. 다음은 **정보보안 스트레스**에 관한 질문 문항입니다.

1. 다음은 귀하께서 인식하고 있는 **보안 관심도**에 관한 질문입니다. 귀하께서 생각하시는 정도에 표시(✔)해 주시기 바랍니다.

No	설 문 내 용	전혀 그렇지 않다	그렇지 않다	보통 이다	그렇다	매우 그렇다
1	정보보안관련 시사뉴스에 관심을 가지고 있다.					
2	다른 직원분들에 비해 정보보안관련 지식이 많다.					
3	보안관련 지식은 나에게 도움이 많이 된다.					
4	동료들과 정보보안에 대한 정보나 소식을 잘 소통한다.					
5	정보보안관련 피해 경험시 다른 동료에게 알려 경고한다.					

2. 다음은 우리회사의 **정보보안 전략 신뢰도**에 관련된 질문입니다. 귀하께서 생각하시는 정도에 표시(✔)해 주시기 바랍니다.

No	설 문 내 용	전혀 그렇지 않다	그렇지 않다	보통 이다	그렇다	매우 그렇다
1	우리회사의 정보보안 전략은 다른 공공기관에 비해 우수하다.					
2	정보보안은 직원들을 대신해서 회사가 알아서 해주어야 한다.					
3	우리회사 정보보안 담당자는 신뢰할 수 있다.					
4	우리회사의 정보보안 전략을 신뢰한다.					
5	우리회사는 정보보안 사고 발생 시 정확한 원인 분석 및 확실한 재발 방지 대책을 수립한다.					

3. 다음은 귀하께서 인식하고 있는 **정보보안 교육수준**에 관한 질문입니다. 귀하께서 생각하시는 정도에 표시(✔)해 주시기 바랍니다.

No	설 문 내 용	전혀 그렇지 않다	그렇지 않다	보통 이다	그렇다	매우 그렇다
1	우리회사는 구성원에게 주기적으로 정보보안 교육 및 훈련을 수행하고 있다.					
2	신입직원에게 적절한 정보보안 교육을 수행하고 있다.					
3	우리회사는 구성원들에게 다양한 방법으로 정보보안 교육을 실시한다.					
4	정보보안 교육은 나에게 꼭 필요한 절차이다.					
5	나는 정보보안 교육을 충분히 받아 업무 대처에 불안감이 없다.					
6	지난 1년간 정보보안 교육에 참여한 시간은 얼마입니까?	( ) 시간				
7	참여한 교육시간은 보안 지식 습득에 충분하다.					

4. 다음은 우리회사의 정보보안 대책으로 인해 귀하께서 느끼시는 **기술적 스트레스**에 관련된 질문입니다. 귀하께서 느끼시는 스트레스 정도에 표시(✔)해 주시기 바랍니다.

No	설 문 내 용	전혀 그렇지 않다	그렇지 않다	보통 이다	그렇다	매우 그렇다
1	내PC지키미의 의무실행으로 인해 부담감을 느낀다.					
2	보안프로그램 사용법이 어려워 불편하다.					
3	빈번한 PC 운영체제 보안 업데이트로 스트레스를 받는다.					
4	최신 기법의 악성메일을 구분하기 힘들어 불안하다.					
5	최신 보안기술 부족으로 해킹사고가 발생할지 몰라 매우 불안하다.					

5. 다음은 우리회사의 정보보안 대책으로 인해 귀하께서 느끼시는 **물리적 스트레스**에 관련된 질문입니다. 귀하께서 느끼시는 스트레스 정도에 표시(✔)해 주시기 바랍니다.

No	설 문 내 용	전혀 그렇지 않다	그렇지 않다	보통 이다	그렇다	매우 그렇다
1	보안USB 사용으로 스트레스를 받는다.					
2	사외 메일 차단에 대한 불편함을 느낀다.					
3	용역업체 직원의 내부 인터넷 사용 통제는 업무 시간 증가의 불편만증가시킨다.					
4	야간이나 주말에 외부인의 정보통신실 출입 통제를 위해 기록을 관리하는 것은 불필요한 일이다.					
5	무선랜(와이파이) 차단은 업무의 불편만 초래할 뿐이다.					

6. 다음은 우리회사의 정보보안 대책으로 인해 귀하께서 느끼시는 **관리적 스트레스**에 관련된 질문입니다. 귀하께서 느끼시는 스트레스 정도에 표시(✔)해 주시기 바랍니다.

No	설 문 내 용	전혀 그렇지 않다	그렇지 않다	보통 이다	그렇다	매우 그렇다
1	분기별 시행하는 사이버 보안 교육으로 스트레스를 받는다.					
2	정보보안 감사·점검·지도방문은 업무에 불편을 초래할 뿐이다.					
3	실제적 보안 활동이 아닌, 형식적인 문서 행정이 반복적으로 지나치게 많다.					
4	매월 시행하는 사이버 보안 진단의 날로 인해 스트레스를 받는다.					
5	빈번하고 복잡한 비밀번호 설정은 업무의 불편만을 초래할 뿐이다.					

Ⅱ. 다음은 귀하의 개인적인 사항에 관한 사항들입니다. 해당되는 곳에 표시(✔)해 주시기 바랍니다.

1) 연 령 : 만 (　　)세

2) 성 별 : ① 남　　② 여

3) 결혼여부 : ① 기 혼　　② 미 혼

4) 최종학력
① 고 졸　　② 전문대졸　　③ 대 졸　　④ 석 사
⑤ 박 사

5) 근무기간 : (　　)년

6) 근 무 지 : ① 사업소　② 본사

7) 근무분야 : ① 사무　② ICT

8) 직　　위
① 일반직원　　② 간　부

★ 설문에 성실히 답변해주셔서 감사드립니다. ★